Cámaras

Tecnologías DE LA Información

Aspectos Jurídicos

Incluye CD-Rom con Certificado Electrónico Camerfirma

Cámaras

Tecnologías DE LA Información

Aspectos Jurídicos

Davara & Davara

Depósito Legal: M - 4243 - 2005

Diseño y preimpresión:
print A porter. Comunicación, S.L.

Impresión: **Imprenta Modelo.**
Salvador Alonso, 12. Madrid

Cámaras

presentación

Si los años ochenta fueron los del decenio de la calidad y los noventa los de la reingeniería de procesos, los primeros del nuevo siglo serán los de la velocidad. De la rapidez con que cambiará la naturaleza de las empresas. De la rapidez con que desarrollarán los intercambios comerciales. De cómo el acceso a la información modificará el estilo de vida de los consumidores y las expectativas planteadas a las empresas. Cuando el aumento de velocidad sea suficiente, la propia naturaleza de las empresas se transformará.

Un nuevo panorama repleto de implicaciones sociojuridícas y económicas derivadas del uso de las Tecnologías de la Información y las Comunicaciones, denominadas por el acrónimo TIC. Del conocimiento y uso que las empresas tengan de algunos aspectos significativos puede depender su ritmo de desarrollo.

Este libro no pretende ser un manual técnico para iniciados. Se trata de explicar a los responsables de las empresas los motivos y consecuencias de un ordenamiento jurídico en torno a las TIC y su uso práctico, para ayudar a resolver determinadas necesidades reales de una sociedad.

El Manual es un acercamiento a cuestiones importantes para la empresa, como la seguridad en las transacciones electrónicas, tanto desde el punto de vista de la firma electrónica como del pago electrónico, las creaciones intelectuales y los nombres de dominio necesarios para la utilización de la Red, la publicidad en Internet, los delitos informáticos, la fiscalidad en el ámbito electrónico o la protección de datos.

Las Cámaras se han involucrado decididamente en un mundo prioritario para la economía. Por ello, han desarrollado servicios básicos de creación de empresas vía Internet, como la Ventanilla Única Empresarial Virtual, el servicio de Certificados Digitales para transacciones entre empresas a través de Camerfirma o una extensa red de herramientas on line *para promover el comercio exterior de las empresas españolas.*

José Manuel Fernández Norniella
Presidente de las Cámaras de Comercio

Cámaras

índice

III. Propiedad Intelectual y nombres de dominio

IV. Otros aspectos de la Sociedad de la Información

V. Fiscalidad en el comercio electrónico

VI. Protección de datos en la empresa

Anexos

abreviaturas

ADR	*Alternative Dispute Resolution*
AEAT	Agencia Estatal de Administración Tributaria
AEPD	Agencia Española de Protección de Datos
art.	Artículo
B2B	*Business to Business*
B2C	*Business to Consumer*
BOE	Boletín Oficial del Estado
CE	Constitución española o Comunidad Europea (según contexto)
CGC	Condiciones Generales de la Contratación
CP	Código Penal
CRM	*Customer Relationship Management*
cc-TLD	*country code Top Level Domain*
DO	Diario Oficial
EP	Establecimiento permanente
ET	Estatuto de los Trabajadores
gTLD	*generic Top Level Domain*
HTTP	*HyperText Transfer Protocol*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IETF	*Internet Engineering Task Force*
IRPF	Impuesto sobre la Renta de las Personas Físicas
IVA	Impuesto sobre el Valor Añadido
LCE	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
LCGC	Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica
LGT	Ley 32/2003, de 3 de noviembre, General de Telecomunicaicones
LOCM	Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos
ODR	*Online Dispute Resolution*
OIT	Organización Internacional del Trabajo
OMPI	Organización Mundial de la Propiedad Intelectual
PKI	*Public Key Infraestructure*
RD	Real Decreto
SET	*Secure Electronic Transaction*
SITAR	Sistema de Información sobre Tramitación Arbitral
SLD	*Second Level Domain*
SSL	*Secure Socket Layer*
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y las Comunicaciones
TLD	*Top Level Domain*
TS	Tribunal Supremo
UE	Unión Europea

introducción

Con la utilización de las Tecnologías de la Información y las Comunicaciones en la actividad jurídica, tanto desde la óptica operativa como del conocimiento, difusión e interpretación de la norma, el profesional jurídico, así como todos aquellos que se ven obligados a tomar decisiones en el ámbito empresarial o a apoyar esta toma de decisiones, necesitan conocer, con precisión y claridad, el papel que estas tecnologías asociadas al ordenador y a las redes de comunicaciones electrónicas juegan en el diario devenir de la empresa para abordar la necesaria adecuación de la operativa diaria a un razonable y controlado conocimiento del riesgo.

Somos conscientes de que el proceso abierto con la utilización de las Nuevas Tecnologías en todos los ámbitos y áreas de actividad, es irreversible. Es por ello, que hay que adaptarse a nuevos métodos para poder retomar los antiguos problemas bajo una óptica diferente y adecuar nuestra actividad al desarrollo tecnológico de forma que el normal desconocimiento que se tiene, en términos generales, de la normativa que gira alrededor de lo que podemos llamar el Derecho de las Tecnologías de la Información y las Comunicaciones (TIC), no provoque riesgos innecesarios o descontrolados, por lo desconocidos, que nos puedan llevar a decisiones empresariales o profesionales desacertadas.

Todo ello conforma la necesidad de un conocimiento de las características básicas de la normativa sobre aspectos tecnológicos que incide directamente en nuestra actividad por el simple hecho de tratar información en forma automatizada y de utilizar la red Internet en la consulta de ficheros y datos y en la simple y muy difundida comunicación a través del denominado correo electrónico.

Pero este conocimiento no es exclusivo del jurista sino que en todos los ámbitos de actividad y, en especial, como decimos, en el de la toma de decisiones, hay que acercarse a un conocimiento mínimo de la normativa sobre las TIC que permita actuar sin riesgos o, al menos, con conocimiento del riesgo en el ámbito de la utilización de la información y su tratamiento automatizado.

Por otro lado, todos sabemos que la información da un gran poder a quien la posee. Surge con ello una nueva clase: la de los poseedores de la información. Pero no es sólo quien tenga la información quien tendrá el poder, sino que hay que saber manejarla, llegando, incluso, a ser más fuerte quien conozca su manejo que quien disponga de ella y no sepa manejarla[1].

[1] *En este sentido se expresa también el informe sobre "La informatización de la Sociedad", conocido como "informe Nora-Minc". Cfr. NORA, S. y MINC, A. "La informatización de la sociedad". Traducción de Paloma García de Pruneda. F.C.E. de España. Madrid. 1983.*

La información es un bien que no se agota con su consumo, sino que, por el contrario, se enriquece con el uso, y ello permite que su expansión se esté produciendo con la creación de más información provocada, en gran medida, por el desarrollo alcanzado en los sistemas de telecomunicación que han permitido que una misma información sea accesible a un número mayor de usuarios.

Al entrar en juego el mundo de las comunicaciones, que con su espectacular desarrollo se une al de la Informática para permitir que el tratamiento automático de la información pueda ser realizado a grandes velocidades y desde cualquier punto, desaparecen las distancias en el tratamiento y transmisión de la información. Empieza a no contar el tiempo ni el espacio.

Se forma así la simbiosis entre la Informática y las Comunicaciones para dar paso al más eficaz tratamiento de la información. La Telemática[2] está cambiando radicalmente la forma de vida. Esta alianza entre las comunicaciones y la informática ofrece una expectativa de prestaciones que hace pocos años podía considerarse de ciencia ficción.

Aunque no somos partidarios de dar más protagonismo del que realmente debe tener a la llamada "red de redes" –Internet–, lo cierto es que, con su masiva utilización, se ha producido un fenómeno social que no nos permite ignorarla. Internet, aunque no sea la única red telemática si es, por su popularización, la más conocida y sirve en muchos casos como muestra o llamada de atención para transmitir un conocimiento o información sobre este particular.

No es necesario incidir más en algo tan evidente y de nada sirve volver la espalda escudándonos en nuestra vocación humanista o nuestra alergia a temas tecnológicos. No hay que confundir las cosas; no se puede vivir ajenos a la realidad, pero, además, la tecnología, en muchos casos, incide directamente en presupuestos humanistas logrando, en la práctica y con su acertada utilización, una auténtica defensa de los derechos de los individuos y, en todos los casos, y sin ninguna duda, una valiosa herramienta para ayudar a recuperar y realizar un efectivo progreso en el sentido humanista de la convivencia social; incluso por encima de intereses mercantilistas o políticos, aunque lo ideal es que esto no fuera necesario y se lograse en paralelo con esos legítimos intereses mercantilistas o políticos.

1. LA DENOMINADA SOCIEDAD DE LA INFORMACIÓN

En la denominada por muchos *Sociedad de la Información,* el valor que se le otorga a ésta es muy importante. Las empresas ya no sólo se valoran en función de los bienes materiales que posean, sino que existe otra parte importantísima que son los bienes inmateriales a los que se sitúa, en muchas ocasiones, con un valor superior al de los activos materiales.

Los Estados, y las organizaciones supranacionales, cada vez toman más en consideración estos activos inmateriales, realizando Proyectos de I+D (actualmente I+D+i, Investigación, Desarrollo e Innovación), y fomentando las creaciones intelectuales en la medida de lo posible.

La nueva economía da más valor a los activos inmateriales que a los materiales. La información, el conocimiento, el fondo de comercio y el uso de la tecnología se han convertido en los puntales de la empresa moderna. Desde esta óptica, nuestro objetivo es dar a conocer los instrumentos de protección necesarios para evitar que cualquier problema relacionado con los activos inmateriales influya en la imagen o en la valoración de una entidad.

La Informática, con las posibilidades que ofrece de almacenamiento y tratamiento de la documentación y la recuperación de la información registrada en soportes magnéticos, ópticos u otros, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control de masas. La unión con las telecomunicaciones agudiza más, si cabe, este aspecto.

[2] *Término fruto de la unión de Telecomunicaciones e Informática que hace referencia al diálogo a distancia entre equipos informáticos.*

En consecuencia, el interés en regular el mundo de la Informática y de las Tecnologías de la Información y las Comunicaciones y de aprovechar sus posibles aplicaciones al Derecho, crece llegando a límites insospechados. El impacto que el nuevo entorno de la información puede tener sobre la sociedad, es tan grande que no nos permite vivir ajenos a él[3].

Es así que, a lo largo de esta obra expondremos muy brevemente las implicaciones jurídicas del uso de las Tecnologías de la Información y las Comunicaciones en la empresa o en la actividad comercial y profesional. El objetivo es llamar la atención sobre las áreas que requieren especial cuidado por ser las que más consecuencias jurídicas implican derivadas de la utilización de dichas tecnologías. Para ello analizaremos las cuestiones relacionadas con la protección de datos de carácter personal, el comercio electrónico y la contratación electrónica, la firma electrónica, la propiedad intelectual e industrial, con especial referencia a los nombres de dominio, los delitos informáticos, y la publicidad en Internet.

2. UN ACERCAMIENTO AL DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Las Tecnologías de la Información y las Comunicaciones no pueden estar ajenas al derecho y es así como en las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las modernas Tecnologías de la Información y las Comunicaciones, surgen los problemas de cómo resolver determinados conflictos nacidos de esa relación.

Así nos encontramos con un nuevo escenario comercial o, expresado de otra forma, un distinto escenario comercial.

Si el avance tecnológico nos ha conducido a un comercio nacional e internacional en el que se incluyen equipos de oficina descentralizados, potentes, con capacidad de procesamiento autónomo y acceso a bases de datos; si las redes de telecomunicación son cada vez más accesibles, más orientadas al servicio y su coste es menor; si la identificación y el procesamiento de la información realizada a través de tarjetas con chip interactivas, han adquirido una dinámica de tratamiento de información que provoca y origina nueva información, lo que permite multiplicar la actividad comercial, era previsible que surgieran, mediante el intercambio de datos entre sistemas, nuevas posibilidades comerciales y aplicación de nuevos métodos de negocio, por otro lado sin tener que producir papeleo y con una dinámica mayor, además de con reducción de tiempo y acercamiento de espacio.

La propia extensión a todas las actividades económicas de las Nuevas Tecnologías de la Información y las Comunicaciones, modifica alguna de las características básicas de la forma de expresarse la oferta y la demanda en los mercados.

Como consecuencia de todo ello, se abren nuevos mercados; o se cierran viejos mercados; o se modifica el mercado; lo podemos llamar como queramos pero, lo que es cierto es que se entra en un ambiente competitivo en el que incluso la empresa o el profesional más renuentes, ante las ventajas que se les presentan o ante el peligro de desaparecer del mercado por su falta de competitividad, preparan sus sistemas informáticos y telemáticos para entrar en el juego de la transferencia electrónica de datos o de la contratación electrónica. Qué duda cabe que se cambian los hábitos en el momento de preparar, de analizar o de realizar un negocio y, en otro caso, es posible que no se pueda competir[4].

Vemos entonces que, sin darnos cuenta y ya en la práctica, se ha creado un escenario de actuación comercial diferente, aunque todavía no sabemos si es beneficioso, o si es, siquiera, conveniente.

---

[3] *El desarrollo tecnológico no puede tomarse como la "panacea", y su aplicación debe de hacerse desde la prudencia. Román Gubern, en su obra "El simio Informatizado", en el último capítulo, bajo el epígrafe "Nuevas Tecnologías y viejos problemas", advierte que las Nuevas Tecnologías no pueden darse como una receta estándar, sino que hay que indagar y preguntarse dónde, en qué contexto, cómo, para qué se aplican, que objetivos persiguen y qué consecuencias inesperadas o involuntarias pueden aparecer. Gubern, Román. "El simio informatizado". Premio Fundesco de Ensayo. Colección Impactos. Madrid. 1987. pp. 207 y ss.*

[4] *Y, por qué no decirlo, también aparecen nuevas posibilidades de actuación fraudulenta.*

3. LA VULNERABILIDAD DE LOS DATOS Y DE LA INFORMACIÓN

Los negocios actuales se han ido creando con una excesiva dependencia de los sistemas informáticos y se han hecho particularmente vulnerables debido, en gran parte, a las características propias del tratamiento telemático.

Vulnerables en principio por la falta de seguridad física que ello conlleva; vulnerables también por la falta de seguridad lógica y vulnerables, por último, por la falta de seguridad jurídica [5]. Porque todas las aparentes ventajas que entraña el tratamiento informático, con la transferencia electrónica de datos y la llamada contratación electrónica, exigen unos presupuestos mínimos de seguridad física y lógica ya sea de equipos, ya sea de sistemas de comunicaciones, ya sea de tratamiento de la información.

La seguridad [6] de los sistemas informáticos y de comunicaciones y, consecuentemente de los datos e información que en ellos se encuentren, o, si se trata de sistemas de comunicaciones, de datos e información que sobre ellos viajan, requieren técnicas, equipos y procedimientos especializados[7].

Las empresas que, por errores o por la actuación de elementos malintencionados, pierden sus datos, sufren graves daños económicos que, en muchas ocasiones, terminan con la quiebra o cierre de la sociedad. De aquí que se busquen protecciones físicas de duplicación de los datos o archivos en diferentes lugares, independientes y distantes entre sí, y protecciones lógicas utilizando complicados métodos y protocolos que efectúan diálogos de control con vistas a la seguridad, sin olvidar, por último, el gran desarrollo que, por este motivo, están teniendo los métodos criptográficos.

En cuanto a la seguridad física y a la seguridad lógica, aún teniendo ambas gran interés, desvían fuertemente la atención del tema fundamental de esta obra y las pasaremos, con esta sencilla referencia, diciendo que se logran equilibrando el sentido común y los conocimientos técnicos, aún a sabiendas de que el uso generalizado de la transferencia electrónica de datos trae como consecuencia un problema de lenguaje, de normas y de compatibilidad entre equipos y programas, para que puedan los ordenadores dialogar entre ellos por medio de las redes de comunicaciones; por otro lado, son estas redes de comunicaciones de diferentes calidades y de diferentes posibilidades, y ello genera dificultades de orden técnico.

A ello hay que añadir que la seguridad y la confidencialidad[8] de los datos no están de otra parte asegurados, en razón a veces, de insuficiencia de medios o de distintas calidades de transmisión de las diferentes redes.

Pero, por si todo esto fuera poco, se plantean dificultades de orden jurídico en la transferencia electrónica de datos y en la contratación electrónica.

---

[5] Respecto a la seguridad jurídica, tenemos que tener en cuenta que, en cuanto sistema normativo, el derecho se manifiesta como sistema de seguridad y como sistema de control social. Desde esta óptica, entenderemos como seguridad jurídica el conjunto de medidas legislativas que protege o cubre los riesgos que el ciudadano corre en la vida ejerciendo su libertad. Sobre la seguridad jurídica, el Profesor SÁNCHEZ AGESTA indica que "en la esfera de la vida moral en cuanto el hombre es un ser libre capaz de decidir sus propias acciones y de escoger sus propios fines, se ha de respetar esta característica de su naturaleza situándolo en condiciones de obrar como un ser libre y responsable. De ello deriva en primer lugar el derecho a una seguridad jurídica en que el hombre adquiere la conciencia y el hábito de su responsabilidad". Esta característica de la libertad del hombre es la que centra nuestro concepto de seguridad jurídica. Cfr. SÁNCHEZ AGESTA, Luis. "Principios de Teoría Política". Madrid. 1967.

[6] Hablamos de seguridad en tres aspectos: Seguridad lógica, seguridad física y seguridad jurídica. Seguridad lógica referida a las posibilidades de protección de los datos registrados en soportes magnéticos, ópticos u otros idóneos para el tratamiento automático, mediante el adecuado empleo de medios informáticos. Seguridad física referida a las posibilidades de protección de esos mismos datos empleando las medidas oportunas de seguridad física y seguridad jurídica en los términos que nos estamos refiriendo a ella. Las dos primeras, seguridad física y seguridad lógica, en principio parecen presentarse como una protección a priori, sin embargo la seguridad jurídica podemos pensar en ella tanto como una protección a priori, mediante el conocimiento del riesgo jurídico en el tratamiento de la información, como una protección a posteriori.

[7] Los equipos y, consecuentemente la información, es vulnerable, por ejemplo, en el caso de haber una pérdida de datos. Es más, las empresas y entidades que más énfasis han puesto en la informatización, llevándola incluso a extremos de dependencia, están especialmente expuestas también a la extorsión y el fraude por mala utilización de estos sistemas.

[8] No se deben confundir los conceptos de "privacidad", "confidencialidad" y "seguridad", referidos a los datos que pueden ser sometidos, o que van a ser sometidos, a tratamiento informático. La "privacidad" hace referencia a que los datos son de una persona y que ésta tiene derecho a controlarlos y a saber como se van a utilizar, la "confidencialidad" se refiere al mayor o menor secreto con que se van a guardar y tratar esos datos, y la "seguridad" hace referencia a las medidas de protección a tomar para la mejor defensa de la privacidad y el grado de confidencialidad.

4. EL POTENCIAL DE PELIGRO DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN

No hemos perseguido más que plantear algunos problemas que ya se están produciendo en la realidad porque, aunque el derecho necesite tiempo para adaptar a los ordenamientos la legislación adecuada al impacto socio-económico de estas tecnologías, el ágil tráfico comercial posee una dinámica diferente y, con su carga de riesgo, utiliza los medios que tiene a su alcance buscando mercados más dinámicos y más rentables. Este tráfico comercial, a veces, no se para a pensar las consecuencias de su actuación en el caso de que, si existieran discrepancias, hubiera que acudir a los órganos jurisdiccionales en busca de soluciones.

La realidad económica y empresarial ha situado a la informática y a las comunicaciones en aquel lugar dónde pueden ser mejor utilizadas. Les corresponde a los juristas estudiar el equilibrio de todos los elementos implicados en el tema para proporcionar ese canto de distribución de justicia dentro de la convivencia social. La búsqueda constante de una convivencia social justa.

Pero, una vez analizados tantos aspectos tecnológicos en el ámbito jurídico, no quisiéramos terminar sin hacer una referencia al potencial de peligro que conllevan las Nuevas Tecnologías y al impacto que pueden tener en el derecho laboral, como cuestión que hoy en día parece tener sensibilizada a una mayor parte de la sociedad y que, evidentemente, tiene una relación directa con el tema que estamos tratando de las posibles implicaciones, desde el punto de vista socio-jurídico, de las telecomunicaciones y las Tecnologías de la Información en la sociedad.

Las facilidades de gestión que proporciona la tecnología, dando rapidez y seguridad al tratamiento de las labores rutinarias en la empresa, lo que es positivo y que, por otro lado, favorece la labor creativa del hombre, ofrece, sin embargo, serias dudas en cuanto a los problemas, por ejemplo, de derecho laboral que se pueden suscitar.

Hay que tener en cuenta, de una parte, que las Nuevas Tecnologías llevan consigo un potencial de peligro desconocido hasta hoy[9], y de otra parte que propician, en la práctica, la sustitución del hombre por la máquina. Esto puede traer un cambio en la normativa laboral; las normas de derecho del trabajo se referirán en el futuro más al mercado del trabajo, si tenemos en cuenta que la tecnología propicia la acortación de la jornada laboral, incluso la variación del lugar de trabajo, y el trabajo en el domicilio, con la modificación de las costumbres sociales y su incidencia en el comportamiento humano.

Y llegamos a una conclusión: siendo evidente el cambio en el ámbito del derecho laboral y de la manifestación de los modos y formas de trabajo, existe la oportunidad de adecuarlo en beneficio de la dignidad humana y de los más elementales derechos del individuo.

5. LAS NORMAS PREMATURAS Y LAS NORMAS REZAGADAS

Para terminar, diremos que, en algunos casos, la falta de regulación de determinados fenómenos informáticos y telemáticos obliga a su definición y protección en una norma donde no tienen su acomodo nato pero que necesita regularlos para poder desarrollar su propio objeto o ámbito de aplicación. Se regula con anticipación –de ahí el nombre que le damos de "norma prematura", en el sentido de adelantada– el fenómeno tecnológico, para poder desarrollar otra situación social que es el verdadero objeto de la norma. Esto hace que sea muy difícil encontrar los lugares en los que se halla regulada la tecnología informática en nuestro ordenamiento, ya que existen normas dispersas que se han visto acogidas por otras que no son acordes con ellas, a veces incluso por su propia naturaleza[10].

[9] *Román GUBERN, en su libro "El simio informatizado", obra digna de estudio, densa e interesante bajo la óptica de buscar un equilibrio entre tecnología y sociedad, a la que ya hemos hecho referencia, llama la atención sobre que existen unos efectos previstos y deseados de las Nuevas Tecnologías y unos efectos imprevistos, similares a veces a los efectos secundarios de los medicamentos. Esto hace pensar que no todo lo que la ciencia y la técnica son capaces de hacer es conveniente que sea hecho. GUBERN, R. "El simio informatizado". op. cit. pp. 207 ss.*

[10] *Estas son las normas que el profesor LOSANO denomina como normae fugitivae, pues "encontrándose allí donde no deberían no son fáciles de hallar, originando una fuente de problemas legislativos". LOSANO, M. "Los proyectos de Ley italianos sobre la protección de los datos personales", en el vol. Problemas actuales de la documentación y la informática jurídica, Tecnos, Madrid, 1987, pg. 279.*

En contraposición a estas normas prematuras se encuentran las normas “rezagadas”, que las llamamos así en el sentido de que surgen después del tiempo oportuno y cuando ya se encuentra una regulación inferior o dispar que ha ido buscando acomodo jurídico de la protección de los derechos de su ámbito. Estas normas han gozado de la oportunidad de aprovechar situaciones y experiencias de otras similares que se encuentran dispersas en el ordenamiento.

El problema surge de las asociaciones entre ellas -prematuras y rezagadas- y en las relaciones de afinidad o rechazo que, a veces, no son contempladas, provocando un caos normativo y contradicciones que conducen al desequilibrio interpretativo así como a la desorientación del jurista.

6. A MODO DE CONCLUSIÓN

El rechazo frontal a la utilización de la informática -las Tecnologías de la Información y las Comunicaciones- y de los medios de “razonamiento” que ofrecen los desarrollos tecnológicos, lejos de descalificar a estos avances técnicos descalifica a los que los rechazan, que ellos mismos se discriminan en su actuación profesional. Afortunadamente, este rechazo ha sido superado en gran parte y se abre el camino –reclamado a gritos en todos los ámbitos jurídicos– de la regulación jurídica del fenómeno informático.

Sin duda que es preciso fijar un marco normativo, técnico y jurídico, adecuado que posibilite la liberalización de las redes y servicios de telecomunicación, con las consiguientes ventajas de abaratamiento de costes de utilización y de acceso a redes y equipos de información estructurados mediante bases de datos y posibilidad de manejo de informaciones de vídeo, voz y datos interactivas que, con una dinámica de utilización, permitiera a cada uno ir adaptándose, de acuerdo con su entorno y posibilidades, a la nueva forma de trabajo y estructura económica, con la creación de un distinto concepto de administración y sistema de formación, con unas líneas maestras, únicas pero flexibles, que pudieran ser utilizadas y aprovechadas por todos.

Pero la necesidad no debe ensombrecer la seguridad; la protección de los derechos de las personas, respecto a su intimidad y confidencialidad, de sus datos o información, que tuviera una consideración y adecuación diferente en el nuevo entorno de la Sociedad de la Información, y la creación de una dinámica de tratamiento de las actividades, que pusiera a disposición del usuario una seguridad física, operativa y, como no, jurídica, son cuestiones básicas a las que hay que prestar máximo interés.

Si existen garantías, si la seguridad se convierte en una prioridad, si se encuentran juntos en tiempo y espacio, aunque sean virtuales, el pago y el comercio electrónicos, en el nuevo escenario comercial, podemos decir que el camino elegido es el adecuado y viajamos con garantías hacia la plena integración en la Sociedad de la Información.

Es una cuestión de seguridad y de confianza; de seguridad de las transacciones respecto a la identificación de las partes y la autenticación de intervinientes en la relación, y del contenido del mensaje.

El gran problema con el que nos encontramos es la falta de conocimiento, formación e información que otorgue la confianza necesaria para el uso de las Tecnologías de la Información y las Comunicaciones y, en particular, para el uso de Internet; se trata de un problema de confianza basado en la falta de seguridad que rodea a la red; falta de seguridad física, falta de seguridad lógica y, cómo no, falta de seguridad jurídica.

capítulo primero

Comercio electrónico

1. INTRODUCCIÓN

La irrupción de las Tecnologías de la Información y las Comunicaciones (TIC) en el ámbito profesional y mercantil está provocando la apertura de nuevos mercados o nuevos campos de actividad así como el cierre de viejos mercados dejando obsoletos algunos campos de actividad; y modificando los mercados y los campos de actividad; lo podemos llamar como queramos pero lo cierto es que se entra en un ambiente competitivo en el que incluso el profesional o la empresa más renuente, ante las ventajas que se le presentan, o ante el peligro de desaparecer del mercado por su falta de competitividad, se prepara para entrar en el juego de la utilización de las Tecnologías de la Información y las Comunicaciones.

Que duda cabe que se cambian los hábitos en el momento de preparar, de analizar o de realizar un trabajo y, en otro caso, es posible que no se pueda competir.

Cualquier profesional, empresa o entidad no solamente utiliza el correo electrónico y lo pone a disposición de todos sus colaboradores, sino que crea su propia página o sitio web en Internet, utilizando un nombre de dominio que, con mayor o menor acierto, proporcione un valor añadido comercial y que identifique e incluso distinga sus productos o servicios de los de los competidores.

La elección y posterior obtención de un determinado nombre de dominio es de gran interés al configurarse como un elemento de marketing y un activo de la empresa. Todos quieren un nombre de dominio que se recuerde con facilidad y que se asocie casi en forma automática a una actividad, persona o empresa de forma que sea fácilmente recordado o encontrado por un buscador cuando se solicite información referente a su negocio[11].

Pero el fenómeno de Internet, y su regulación jurídica, no está centrado solamente en la problemática y gran valor de los nombres de dominio sino que extiende su radio de acción a cuestiones tan o más importantes como, por ejemplo, el acceso a conteni-

[11] *Los nombres de dominio se han constituido en un activo inmaterial muy valioso para las entidades, lo que ha dado lugar, en no pocas ocasiones, a supuestos de negociación con quien había registrado con carácter previo un nombre de dominio que luego resultaba ser de interés para una entidad que se veía abocada a pujar para conseguirlo, debido al principio de prioridad temporal que se sigue en la asignación, el conocido "first come, first served", es decir, que el primero que registre un nombre de dominio, en principio, se lo queda, restando únicamente el recurso ante la ICANN (Internet Corporation for Assigned Names And Numbers, entidad encargada del registro y asignación de nombres de dominio), o sus organismos delegados para que se resuelva, en caso de controversia, para recuperar un nombre de dominio al que se cree se tiene derecho. No obstante, no queremos extendernos más aquí y nos remitimos al apartado que más adelante dedicamos a esta materia.*

dos, proporcionar información comercial, en texto, sonido e imagen a través de la red, estructurar campañas de marketing y prospección comercial utilizando la telemática, contratar por medios electrónicos, facturar con la utilización de medios tecnológicos y tantas otras cuestiones que harían interminable un primer acercamiento al conocimiento de la regulación jurídica de Internet.

Esta regulación jurídica ha comenzado hace ya tiempo y se ha mostrado, en su primera manifestación material en nuestro ordenamiento jurídico, con la promulgación de la denominada Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico [12], más corrientemente conocida como la Ley de Comercio Electrónico (LCE).

Con la aprobación de la LCE, se abre una etapa que tiende hacia la regulación jurídica de Internet y de todos aquellos aspectos [13] que giran alrededor del denominado comercio electrónico y que, por su utilización real y su implicación práctica no se pueden demorar más.

Es así que esta Ley afecta a todos los que, desde una óptica profesional o mercantil, con un contenido económico, directo o indirecto, estamos en Internet y permitimos el acceso a nuestra información, aunque sea de una forma gratuita, a aquellos que lo solicitan conectándose a nuestra página o sitio web.

Es, por tanto, una Ley que afecta a todos los que estamos en Internet, los que tenemos u ofrecemos información por la red, y todos debemos conocerla.

Con la promulgación de esta Ley algunos han llegado a decir que ya existe una norma que regula Internet. Pero, en nuestra opinión, esto no es así.

Ni Internet representa un fenómeno tan simplista como para poder ser regulado por una única norma específica, ya que afecta a diversas áreas o ramas del propio Derecho, ni Internet representa un fenómeno tan complejo que necesite una dedicación más exhaustiva que la de cualquier otra relación jurídica similar, por mucho que incida sobre la materia el particular medio de comunicación.

Internet es una realidad social que el Derecho no puede desconocer y, en consonancia con ello, configura un entorno económico que demanda una regulación jurídica que proporcione la seguridad necesaria para poder operar en la red con garantías.

La LCE viene a regular temas tan polémicos como la presencia de una empresa u organización en Internet, desde aspectos sencillos como puede ser una simple comunicación comercial, hasta cuestiones más o menos problemáticas que inciden incluso en múltiples relaciones mercantiles como, por ejemplo, la contratación de bienes o servicios por vía electrónica, el suministro de información por vía telemática o, por no seguir enumerando todos y cada uno de los Servicios de la Sociedad de la Información, el ofrecimiento de instrumentos de búsqueda, acceso y recopilación de datos y transmisión de información a través de una red de telecomunicaciones.

Es evidente que el comercio electrónico, entendido en un sentido amplio, y la contratación electrónica en general y, en particular, la realizada a través de la red, exigen seguridad jurídica.

La LCE puede representar un buen punto de partida para ofrecer y proporcionar esa seguridad jurídica que tanto necesitan los actos de comercio efectuados a través de Internet.

---

[12] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, publicada en el Boletín Oficial del Estado número 166, de 12 de julio; en adelante LSSI o, también, LCE. Y corrección de error publicada en el Boletín Oficial del Estado número 187, de 6 de agosto de 2002.

[13] Múltiples aspectos con indudables repercusiones jurídicas como, por ejemplo, todas las cuestiones relacionadas con el derecho fundamental a la protección de datos, la contratación informática, la contratación electrónica, la publicidad por la red, los nombres de dominio, la validez y eficacia jurídica de los documentos generados por estos medios telemáticos, la utilización de las comunicaciones electrónicas en las relaciones administrado y Administración, en los procedimientos administrativos y jurisdiccionales, y otras muchas más que pensamos no es el momento de analizar.

2. CONCEPTO DE COMERCIO ELECTRÓNICO Y DE CONTRATACIÓN ELECTRÓNICA

En un primer acercamiento, por comercio electrónico podemos entender tanto la compra de productos o servicios por Internet, como la transferencia electrónica de datos entre operadores de un sector en un mercado, o el intercambio de cantidades o activos entre entidades financieras, o la consulta de información, con fines comerciales, a un determinado servicio, o un sinfín de actividades de similares características realizadas por medios electrónicos; pero, para no perdernos en ambigüedades, entenderemos, en un sentido amplio, que es comercio[14] toda aquella actividad que tenga por objeto o fin realizar una operación comercial, y que es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando.

El hecho de estar en Internet añade obligaciones nuevas a las que ya se tienen que cumplir como comerciante. Esto es una característica que no puede obviar el hecho de que nos encontremos ante una forma de comercio que como tal debe cumplir con todas las obligaciones que se desprenden de la actividad comercial y que se derivan del Código de Comercio y del Código Civil además de, en su caso, las leyes especiales que en cada caso corresponda aplicar.

Pero, en particular, centraremos nuestra atención en la LCE, ya citada, que supone un régimen específico del comercio electrónico que no sustituye sino que se añade al régimen legal de las actividades comerciales.

El adjetivo de electrónico no añade al comercio otra característica que la de desarrollarse empleando herramientas electrónicas en todas o en una parte de sus fases de celebración.

Dejando el concepto de comercio electrónico, y entrando en el de la contratación electrónica, diremos que entendemos por contratación electrónica aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo.

Cada día son más los negocios que se realizan utilizando estos medios electrónicos y cada vez son más aceptados de hecho –si no de derecho– en nuestra sociedad. Pero, con este tipo de contratación, en muchas ocasiones, surgen dificultades, tanto de orden jurídico como de orden técnico.

Respecto a la utilización del comercio electrónico, desde el punto de vista del que realiza la oferta en la contratación, podemos decir que una empresa está realizando una actividad de comercio electrónico cuando contempla la utilización de estos medios (de los electrónicos, en general, y de la red, en particular), como un canal de comercialización de su oferta, de productos o servicios, habiendo adaptado esta oferta, incluidas las políticas comerciales y el precio[15], a las características peculiares de la utilización de la electrónica y de la red.

Ello exige una adaptación del comportamiento y forma de trabajo del comerciante a las características del "escaparate" que es la red y, además, adaptar también su actividad, cuando ello sea posible, a otros o distintos canales de distribución.

En todo comercio electrónico debe existir un canal de distribución electrónico que, en algunos casos, deberá ser completado con un canal de distribución tradicional que permita hacer llegar los bienes y productos que se han contratado desde el productor[16], o desde el distribuidor, hasta el usuario; el canal

---

[14]Cualquier acto de comercio –entendiendo por tal los comprendidos en el Código de Comercio y cualesquiera otros de naturaleza análoga (artículo 2 del Código de Comercio)-, realizado por medios electrónicos en el sentido que exponemos, será considerado, a los efectos que tratamos, como comercio electrónico; queremos decir con ello que no es solamente la compraventa electrónica el objeto de nuestro estudio en el tema del comercio electrónico.

[15]Hay que tener en cuenta que al utilizar la red se están usando unos canales diferentes de comunicación y de oferta con el futuro comprador que, en ocasiones, pueden abaratar el producto al no necesitar unas estructuras y gastos de locales y otros que son necesarios en la contratación convencional.

[16]Como es natural, la distribución de los productos o bienes tangibles no se puede realizar virtualmente, a través de la red, pero existen medios y ofertas de seguimiento del paquete o envío sabiendo en todo momento dónde se encuentra y el recorrido que está haciendo por la empresa de distribución, así como la predicción de llegada y momento de entrega que se adecuará a las necesidades del propio usuario.

de distribución que en sí puede ser la red solamente se configura como un canal de distribución de datos o de información en los que se puede o no incluir un compromiso –compromiso electrónico– que deberá reunir unas determinadas características[17].

Con relación al desarrollo y situación actual, es evidente su utilización que aumenta, día a día, en forma exponencial, en todos los tipos y formas de comercio incluidos aquellos que pudiera parecer que, por su naturaleza, no se prestan bien a ser ofertados, desarrollados y, mucho menos, completados en todas sus fases, a través de Internet.

Las aplicaciones de comercio electrónico, de compra por Internet, en supermercados, grandes almacenes, banco en casa, oferta de productos por la red, etc., se observa cómo crecen en periodos pequeños de tiempo, no siendo necesario acudir a cifras que, por un lado nadie conoce bien su fiabilidad, y, por otro lado, todas destacan el ascenso de operaciones y volumen de las mismas cuando se realiza la acción a través de la red.

3. CLASES DE COMERCIO ELECTRÓNICO

La clasificación del comercio electrónico podemos analizarla desde dos puntos de vista, uno objetivo, atendiendo a los medios utilizados en su desarrollo y otro subjetivo, atendiendo a los sujetos intervinientes en el mismo.

Desde el punto de vista objetivo, partiremos de la cobertura que otorgue la utilización de medios electrónicos, es decir, atendiendo al total o parcial desarrollo del acto de comercio por vías electrónicas. De este modo, diferenciamos el **comercio electrónico directo** o comercio electrónico *on line,* del **comercio electrónico indirecto** o comercio electrónico *off line.*

El comercio electrónico directo, o comercio electrónico *on line,* es aquél que se desarrolla por completo por medios electrónicos. Nos estamos refiriendo al comercio de bienes y/o servicios digitalizados: esto es, desde la contratación de un viaje en el que se envía un billete electrónico por red, hasta los ejemplos habituales de compra de productos informáticos, libros electrónicos o discos, música digital. En este caso, todas las fases se realizan a través de medios electrónicos.

Por su parte, **el comercio electrónico indirecto,** o comercio electrónico *off line,* implica el empleo conjunto de medios electrónicos y no electrónicos en su desarrollo. Por ejemplo, puede iniciarse por medios electrónicos pero requerir de medios físicos para terminar, es decir, no se puede completar la transacción electrónicamente, pongamos por caso, la distribución de mercancías físicas.

Atendiendo a los sujetos intervinientes podemos distinguir los siguientes agentes en el comercio electrónico: Administraciones (A), las empresas (B) y los consumidores (C).

El comercio electrónico puede derivar de una relación comercial[18] entre cualesquiera de estos agentes comerciales entre sí, de modo que distinguimos las siguientes combinaciones:

	A	B	C
A	A2A	A2B	A2C
B	B2A	B2B	B2C
C	C2A	C2B	C2C

[17]La distribución de información a través de la red reúne unas peculiaridades, por su posibilidad de cambio y su dinámica, que ofrece ventajas e inconvenientes.

[18]Entendemos relación comercial en sentido amplio y sin ceñirnos al formalismo del término, lo que nos permite abarcar todas las relaciones que exponemos con el fin de centrarnos solamente en la característica de realizarse por medios electrónicos.

- **A2A:** transacciones entre Administraciones. Cualquier clase de relación entre organismos pertenecientes a la Administración, entendida en sentido amplio porque incluye el poder legislativo, el ejecutivo y el judicial, realizada por medios electrónicos.
- **A2B:** transacciones electrónicas desde la Administración hacia las empresas.
- **A2C:** transacciones electrónicas desde la Administración al consumidor/administrado.

- **B2A:** transacciones electrónicas desde las empresas a la Administración.
- **B2B:** transacciones electrónicas entre empresas.
- **B2C:** transacciones electrónicas entre empresas y consumidores.

- **C2A:** transacciones electrónicas entre consumidor/administrado y Administración.
- **C2B:** transacciones electrónicas entre el consumidor y la empresa.
- **C2C:** transacciones electrónicas entre particulares/consumidores.

4. CARACTERÍSTICAS DEL ENTORNO ELECTRÓNICO

El nuevo escenario comercial que ha surgido, como consecuencia de la contratación electrónica, obliga al tráfico mercantil a utilizar medios electrónicos y de comunicaciones para aprovechar las oportunidades del mercado, y la práctica hace que se den como buenas las voluntades, independientemente del lugar donde han sido emitidas y el medio por el que se han realizado, y también sin considerar si se trata de un contrato civil o mercantil [19].

Es así que podemos decir que en el comercio electrónico suele entrar en juego un elemento diferenciador que le otorga algunas características que deben ser analizadas: nos referimos a las redes de comunicaciones y, en particular, a Internet.

Es imposible tratar este tema sin tener en cuenta que los problemas surgen, en casi todos los casos, al incidir las comunicaciones –unidas, eso sí, a la electrónica y al tratamiento automático de la información– en la relación contractual que estamos analizando.

La posibilidad de transmitir datos o información en grandes cantidades, superando los clásicos inconvenientes de tiempo y distancia, condicionan algunas de las teorías en las que se ha basado, tradicionalmente, el análisis de la contratación.

Es necesario, por tanto, hacer referencia a los medios de comunicación y a la influencia que pueden tener, desde el punto de vista legal, en la operación o actividad comercial que estemos tratando.

Pero, al actuar los medios de comunicación y las características del entorno electrónico pueden surgir dudas sobre la seguridad de la transacción o actividad que se desarrolla.

La seguridad es un tema que adquiere gran trascendencia, desde el punto de vista de la garantía jurídica, por ejemplo, en la formación de los contratos.

Pero esta seguridad debe ser analizada desde tres ópticas, ya que, en la transmisión por medios electrónicos –sean o no telemáticos, pero en forma más agudizada en los telemáticos– se necesita concretar la persona o identidad del emisor, el contenido de la información o datos que se transmiten y la persona o identidad del receptor.

---

[19] En la actualidad, en muchos casos, se están aceptando ofertas hechas por fax por el mismo medio -el fax- y se espera la ejecución del contrato con el convencimiento de que la contratación se ha perfeccionado. La propia competencia, y la necesidad de entrar en un mercado insolente, hace que se realicen operaciones en cadena, tomando como buena la ejecución de un contrato aceptado en cuanto a la voluntad por uno de estos medios, cuando es posible que, por un simple error tecnológico o de comunicaciones, no haya llegado la aceptación a su destino, incluso, es posible que nunca llegue.

Al mostrar un documento emitido por medios electrónicos, en principio y por sí solo, no se puede asegurar quiénes son las partes (identificación) y si existe o no total coincidencia entre el contenido del mensaje enviado y el contenido del mensaje recibido (integridad). Es por ello que debemos independizar estos aspectos y tratarlos por separado.

5. LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

Para conocer el entorno del comercio electrónico debemos partir del concepto de "Servicios de la Sociedad de la Información".

Servicios de la sociedad de la información o servicios: *todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.*

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios (aptdo. a) del Anexo de la LCE).

Si nos detenemos a analizar esta definición comprobamos que son cuatro las características que encuadran a un servicio como de la Sociedad de la Información:

- Servicio prestado normalmente a **título oneroso:** como ya se indica a continuación, 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. En este sentido se entiende por ejemplo que si una página web está sustentada o patrocinada, este servicio es oneroso aunque el coste no lo soporte el destinatario final; dado que reporta un ingreso o beneficio para el prestador de servicios.
- **A distancia:** es decir que la prestación de servicios se realiza sin presencia física simultánea de prestador y destinatario en el mismo lugar.
- **Por vía electrónica:** esto es, con el uso de medios electrónicos en la prestación.
- **A petición individual del destinatario:** primando así, en todo Servicio de la Sociedad de la Información, la voluntad del destinatario de recibirlo previa solicitud y respetando en todo momento su libertad de elección.

En este concepto de *Servicios de la Sociedad de la Información,* se incluyen desde los servicios más amplios que se pueden prestar a través de la red, como puede ser la contratación de bienes y servicios por vía electrónica, hasta la simple facilitación de búsqueda o enlaces a otros sitios de Internet [20].

Este amplio abanico incluye por ejemplo, el suministro de información por dicho medio, las actividades de intermediación relativas a la provisión de acceso a la red, la transmisión de datos por redes de telecomunicaciones, 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 facilita-

---

[20] *Expresamente señala el apartado a) del Anexo de la LCE que "No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:*

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994,de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas".

dos por otros o 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 destinatarios.

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.

Establecido el concepto de Servicio de la Sociedad de la Información, es necesario diferenciarlo de lo que la LCE denomina *servicios de intermediación,* que son servicios a través de los que se facilita la prestación o utilización de otros Servicios de la Sociedad de la Información o el acceso a la información, como, por ejemplo, los servicios de telecomunicaciones o comunicaciones electrónicas que permiten el acceso a Internet, los de alojamiento o almacenamiento *(hosting)* de datos en servidores de Internet, o los enlaces a contenidos o instrumentos de búsqueda, como los portales o motores de búsqueda de Internet.

En conclusión, el concepto de Servicio de la Sociedad de la Información que proporciona la LCE es muy amplio, pudiendo considerarse un gran número de actividades como tal, y quedando, por tanto, sujetas al régimen jurídico previsto por la Ley, lo que supone que el prestador de servicios, sea persona física o jurídica, tenga que cumplir con las obligaciones que la misma le impone.

La regulación de los Servicios de la Sociedad de la Información se lleva a cabo por la LCE, que tiene por objeto establecer el régimen jurídico de los Servicios de la Sociedad de la Información y de la contratación por vía electrónica en los diversos aspectos enumerados en su artículo 1, tales como las obligaciones de los prestadores de servicios en la transmisión de contenidos, el régimen jurídico de las comunicaciones comerciales que se envíen por correo electrónico u otro medio de comunicación electrónica equivalente o el régimen sancionador que es de aplicación a los prestadores de servicios.

Por expresa disposición de la LCE, quedan excluidos de su ámbito de aplicación diversos servicios, que se regirán por su normativa específica. Éstos son los servicios:

- prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas,
- que tengan por objeto medicamentos y productos sanitarios,
- prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

Esto supone afirmar que si un abogado tiene un sitio o página web mediante el que proporciona información, bajo su responsabilidad profesional, a los que se conectan o consultan el mismo, será considerado como prestador de servicios conforme a la LCE, teniendo que cumplir con sus disposiciones, salvo en lo que se refiere a su actuación de representación y defensa en juicio.

Por último, cabe señalar que la prestación de Servicios de la Sociedad de la Información en España, conforme al principio de libre prestación de servicios establecido por la Directiva 2000/31/CE[21], no se encuentra sujeta a autorización administrativa previa. Este principio ha de entenderse sin perjuicio de las autorizaciones que el prestador de servicios requiera para el desarrollo de su actividad, previstas en el ordenamiento jurídico, y que no se refieran de forma específica a la prestación del servicio por vía electrónica, y en especial de Internet.

[21] *Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), publicada en el Diario Oficial serie L, núm. 178, de 17 de julio.*

6. PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

*"**Prestador de servicios o prestador:** persona física o jurídica que proporciona un servicio de la sociedad de la información"* (aptdo. c) del Anexo de la LCE).

El concepto de Prestador de Servicios de la Sociedad de la Información ha de entenderse en sentido amplio, incluyendo a los que prestan también servicios de intermediación, pero distinguiendo en el régimen de actuación de los mismos obligaciones diferentes para unos y para otros.

Puede darse el caso de que una entidad actúe como prestador de servicios y a la vez como prestador de servicios de intermediación. En este supuesto habrá que distinguir entre sus actuaciones, cuáles son de prestador de servicios y cuáles de prestador de servicios de intermediación, con el fin de asociarle unas u otras obligaciones.

Con carácter general, como ya hemos indicado, la prestación de servicios dentro de la Sociedad de la Información se rige por el principio de libre prestación, lo que implica que no es necesaria ninguna autorización previa para poder prestar servicios en el ámbito de la denominada Sociedad de la Información, sin perjuicio de los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.

	PRINCIPIO DE LIBRE PRESTACIÓN DE SERVICIOS
Prestación de servicios	La actividad de los prestadores de servicios: – no está sujeta a autorización previa, – sin perjuicio de los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo los servicios de la sociedad de la información.
Principio de libre prestación de servicios	La prestación de servicios que procedan de: – un prestador establecido en algún Estado miembro de la Unión Europea[22], o – del Espacio Económico Europeo[23] – se realizará en régimen de libre prestación de servicios, – sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto: • los supuestos legalmente previstos, y • el respeto a principios fundamentales de la convivencia social.
Restricciones a la prestación de servicios	– la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional, – la protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores, – el respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y – la protección de la juventud y de la infancia.

[22]Países de la Unión Europea (UE): Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Irlanda, Italia, Luxemburgo, Países Bajos, Portugal, Reino Unido, Suecia, a los que en el 2004 se han sumado Chipre, República Checa, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, Eslovaquia y Eslovenia.

[23]Países del Espacio Económico Europeo (EEE): Países de la UE y Noruega, Islandia y Liechtenstein.

Desde una perspectiva territorial, con carácter general, la LCE se aplica de un lado, a los prestadores de servicios **establecidos en España** y de otro, a aquéllos que sin ser residentes en España, prestan Servicios de la Sociedad de la Información a través de un **establecimiento permanente** situado en España.

No obstante, la LCE también será de aplicación, en algunos casos, a los prestadores establecidos en otros Estados miembros de la Unión Europea o del Espacio Económico Europeo y también, en determinadas circunstancias, a prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.

a. Prestadores de servicios establecidos en España

Se entiende que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

La LCE también será de aplicación a los Servicios de la Sociedad de la Información que se ofrezcan por prestadores residentes o domiciliados en otro Estado a través de un establecimiento permanente situado en España. En este sentido, se considera que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

Hay que tener en cuenta que se presumirá que el prestador de servicios está establecido en España cuando éste o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro Registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica, sin embargo, la mera utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

Como ya hemos reiterado, todos los Prestadores de Servicios de la Sociedad de la Información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

b. Prestadores de servicios establecidos en otro Estado de la Unión Europea o del Espacio Económico Europeo

Sin perjuicio del principio de libre prestación de servicios y de las restricciones que, en su caso, puedan existir a la prestación de servicios, la LCE también se aplicará a los prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las siguientes materias:

- Derechos de propiedad intelectual o industrial.
- Emisión de publicidad por instituciones de inversión colectiva.
- Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.
- Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.
- Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.
- Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

En caso de bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español, por ejemplo, requisito de escritura pública e inscripción en el Registro de la Propiedad, en su caso, todo lo que se refiera a la constitución, transmisión, modificación y extinción de derechos reales sobre los mismos.

Los prestadores de servicios que suministren servicios relacionados con las materias anteriores igualmente se someterán a las normas del ordenamiento jurídico español que las regulen. No obstante, la LCE no será de aplicación en el supuesto de que en virtud de las normas reguladoras de estas materias no fuera aplicable la ley del país en que resida o esté establecido el destinatario del servicio.

c. Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo

Respecto de los prestadores de servicios establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo habrá que atender, en lo que se refiere al principio de libre prestación de servicios, a los acuerdos internacionales que resulten de aplicación.

Asimismo, respecto de estos prestadores, los organismos competentes podrán adoptar las medidas necesarias para que se interrumpa la prestación de un servicio o para retirar los datos que vulneren, atenten o puedan atentar contra los siguientes principios:

– la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional,

– la protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores,

– el respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social,

– la protección de la juventud y de la infancia.

En relación con los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos a las obligaciones previstas en la LCE, siempre que ello no contravenga lo establecido en los Tratados o Convenios internacionales que sean aplicables.

d. Prestadores de servicios de intermediación

Los prestadores de servicios de intermediación también están sometidos a la LCE, según se desprende del artículo 1.1 que establece que el objeto de la LCE es la regulación del régimen jurídico de los Servicios de la Sociedad de la Información y de la contratación a través de medios electrónicos en lo relativo a las obligaciones de los prestadores de servicios, incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones.

La LCE distingue cuatro tipos de prestadores de servicios de intermediación:

- Los operadores de redes y servicios de comunicaciones electrónicas y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a la red de telecomunicaciones, incluyendo estas actividades de transmisión y provisión de acceso el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.
- Los prestadores que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a

otros destinatarios que lo soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal.

- Los prestadores de servicios de alojamiento o almacenamiento de datos cuyo servicio de intermediación consiste en albergar datos proporcionados por el destinatario del servicio.
- Los que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos.

Como obligaciones específicas de los prestadores de servicios que presten servicios de intermediación, los artículos 11 y 12 de la LCE recogen las de colaboración y retención de los datos de tráfico.

7. PRESENCIA EN INTERNET

Un prestador de servicios puede estar presente de varias formas en la red: de un lado, puede presentarse solamente de una manera estática, esto es, simplemente "estando en Internet", mediante una presencia que se limita a ofrecer información sobre su actividad e identificación sobre su identidad, dirección u otras y, de otro lado, puede llegar incluso a realizar contratación electrónica por la red, pasando por diferentes estados intermedios que se pueden contemplar.

Vamos a analizar las consecuencias jurídicas derivadas en cada caso.

a. Presencia estática

Tendrá una presencia estática quien se presente en Internet efectuando labores relativas al comercio electrónico en el sentido que hemos analizado, es decir, cuando desarrolle actividades comerciales que tengan o puedan tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando.

Puede consistir solamente en ofrecer información sobre su identidad, dirección y contenido de los productos o servicios que ofrece, pero de una forma que denominamos 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.

b. Presencia dinámica

Si hemos definido a los prestadores de servicios con presencia estática como los que no interrelacionan con el destinatario de la información más que, en su caso, en el seguimiento de instrucciones de navegación comprendidas en la página web, los prestadores de servicios que tienen una presencia dinámica serán, en contraposición, los que 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 la presencia dinámica podemos diferenciar, por tanto, la presencia solamente conversacional y la contractual.

b.1. Conversacional

La presencia dinámica conversacional es aquélla en la que el servicio que se ofrece va más allá de la simple información pero no llega a suponer una contratación electrónica, es decir, se trata de un prestador de servicios intermedio entre el estático y el dinámico contractual, por ejemplo, un prestador que ofrece un diálogo con el usuario sin llegar a posibilitar una verdadera contratación electrónica, como por ejemplo un servicio de asesoramiento sobre la utilización de un producto o servicio.

Se llegan a establecer en estos casos conversaciones electrónicas de simulación de ofertas o servicios que pueden afectar, incluso, a cuestiones de competencia.

b.2. Contractual. Contratación electrónica

El segundo supuesto de presencia dinámica de los prestadores de Servicios de la Sociedad de la Información es, como ya hemos indicado, el de la presencia contractual.

"Contrato celebrado por vía electrónica o contrato electrónico: *todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones"* (aptdo. h) del Anexo de la LCE).

b.2.a) Validez y eficacia

En primer lugar, la celebración de contratos por vía electrónica no necesita la admisión expresa de esta técnica –produciendo todos los efectos previstos en el ordenamiento jurídico cuando concurran el consentimiento y los demás requisitos necesarios para su validez (al menos también objeto y causa)–, ni que las partes acuerden previamente la utilización de estos medios electrónicos.

Es decir, los contratos electrónicos se regirán, como ya hemos indicado, además de por la LCE[24], por lo dispuesto en el Código Civil y en el Código de Comercio y demás normas específicas en concreto, sin olvidar especialmente, en su caso, las normas de protección de los consumidores.

Siempre que en la ley se exija, en cualquier contrato, que se celebre por escrito para su validez, este requisito de escritura se entiende cumplido si el contrato o la información se contiene en un soporte electrónico. Esto supone un respaldo legislativo mayor a la figura del documento electrónico que ya tenía un importante soporte en diferentes normas de nuestro ordenamiento jurídico[25].

El valor que normalmente tiene la firma de un documento en nuestro entorno social es el de asociar el contenido de ese documento a la voluntad de la persona autora de la firma, es una garantía de fiabilidad entendida como imposibilidad de copia. Esto ocurre en los documentos que se encuentran en soporte papel y que, por tanto, la firma es manuscrita. Si es así en la firma manuscrita, mucha más garantía y fiabilidad aporta la firma electrónica[26].

b.2.b) Prueba

En cuanto a la prueba de la celebración de un contrato por vía electrónica hay que destacar que será admisible en juicio como prueba documental el soporte electrónico en el que se encuentre un contrato celebrado electrónicamente.

El régimen jurídico de la prueba de la celebración de contratos electrónicos y de las obligaciones que de ellos se deriven se sujetará a las reglas generales del ordenamiento jurídico y, en su caso, a lo previsto por la legislación de firma electrónica.

Ya hemos hecho referencia al reconocimiento de eficacia jurídica del documento electrónico y a su admisión como prueba documental. Como documentos electrónicos podemos diferenciar dos clases. De una parte el documento en soporte papel cuyo contenido haya sido generado por medios electrónicos y de otra parte el documento en soporte electrónico cuyo contenido haya sido generado por medios electrónicos.

---

[24] En particular, por lo previsto en su Título IV, a excepción de aquellos contratos que se refieran al Derecho de familia y sucesiones que no les será de aplicación lo dispuesto en ese Título IV de la LCE. Además, se regirán por su legislación específica los contratos en los que la ley acuerde para su validez o para la producción de determinados efectos la forma documental pública o que requieran la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas.

[25] Como simple apunte, podemos referenciar el art. 230 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, el art. 45.5 de la Ley 30/1992, por la que se regula el Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, el art. 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica o el art. 26 del Código Penal.

[26] A este respecto y como llamada de atención, diremos que la firma manuscrita es fácilmente copiable o imitable; por el contrario, la firma electrónica, basada en criptografía de clave asimétrica resulta prácticamente imposible de copiar o falsificar.

Ambos tipos de documentos son frecuentemente utilizados y, en ocasiones, necesarios para poder desarrollar una actividad comercial, empresarial e incluso profesional. Pensemos por ejemplo en la venta por medio de tarjetas de crédito, o cualquier otra transacción por medio de tarjetas de débito, en las que el documento que sale impreso en un terminal punto de venta, o por un elemento informático, y ha quedado dicho original registrado en un soporte informático. El usuario firma esta factura o justificante aceptando la validez de lo en él expresado que, como hemos dicho, es copia impresa de un original electrónico generado por un procedimiento informático. Además esta aceptación puede hacer que la operación quede totalmente cumplimentada, pago y abono, y sobre ellas se realicen otra serie de operaciones en cadena, dando validez con ello a la conformidad en forma electrónica de la operación.

Para poder acudir a estos documentos se hace necesario establecer garantías respecto a la fiabilidad del contenido y a la seguridad de su almacenamiento, de este modo los sistemas informáticos tendrán que ofrecer unas medidas de seguridad y de control ante el acceso no autorizado, así como garantizar la confidencialidad de la información en los casos en que sea exigible.

Todas estas medidas son tendentes a garantizar la conservación de los originales y la no modificación o alteración de los contenidos. Ocurre igualmente en los documentos en soporte papel, que también requieren las medidas para garantizar la no modificación de los contenidos, así por ejemplo la necesidad de su firma o de marcas de control para evitar que se pueda escribir a partir de un lugar determinado. Estas medidas y otras en ocasiones mejores, como las técnicas criptográficas aplicadas al documento en soporte informático, les hacen más seguros e inaccesibles a su modificación y alteración que documentos en soporte papel. La falsificación y alteración fraudulenta de la documentación en soporte papel ha llegado a unas técnicas de perfeccionamiento que es muy difícil se logren con tanta facilidad en soportes informáticos.

b.2.c) Intervención de terceros de confianza

Las partes podrán pactar que un tercero archive en soporte informático las declaraciones que hubieran tenido lugar por vía electrónica y que integran los contratos electrónicos, consignando la fecha y la hora en que tuvieron lugar. El tercero archivará las declaraciones que hubieran tenido lugar por vía telemática entre las partes por un período estipulado no inferior a cinco años.

La intervención de estos terceros para archivar las declaraciones que por vía electrónica hayan tenido lugar entre las partes no podrá alterar ni sustituir las funciones que corresponden a las personas facultadas para dar fe pública.

b.2.d) Lugar y momento de celebración

A efectos de determinar el régimen jurídico aplicable y considerando que la contratación electrónica ofrece la posibilidad de celebrar contratos a distancia –de hecho toda la contratación por Internet es contratación a distancia–, se hacen necesarias unas reglas que determinen dónde ha de entenderse celebrado el contrato en cada caso.

B2C: residencia consumidor

Los contratos celebrados por vía electrónica en los que intervenga un consumidor como parte se van a presumir celebrados en el lugar donde el consumidor tenga su residencia habitual.

B2B: establecimiento del prestador de servicios (PS)

Los contratos electrónicos entre empresarios o profesionales se presumirán celebrados en el lugar en que esté establecido el prestador de servicios, salvo que las partes pacten algo diferente.

Respecto al momento en el que se entienden celebrados los contratos su importancia radica en que puede determinar el inicio de la producción de sus efectos, esto es el momento en el que las obligaciones de las partes comienzan a ser exigibles y deben ser cumplidas.

Los contratos electrónicos se caracterizan por celebrarse estando las partes contratantes en lugares diferentes. Este hecho resalta la importancia de determinar el momento en que se entiende que el contrato comienza a producir efectos. La contratación entre ausentes tradicional (por carta, por fax) ha traído consigo este problema y la LCE ha venido de algún modo a determinar el momento exacto en el que se entiende celebrado el contrato.

Así dispone que en los contratos celebrados mediante dispositivos automáticos *"hay consentimiento desde que se manifiesta la aceptación",* supone esto que el contrato comienza a producir efectos desde que se acepta.

A este respecto, la LCE modifica el Código Civil y el de Comercio unificando así el criterio de determinación del momento en el que se entiende celebrado el contrato cuando intervienen dispositivos automáticos [27].

8. OBLIGACIONES DERIVADAS DE LA PRESENCIA EN INTERNET

Distinguiremos dos casos dependiendo de la presencia de la entidad en Internet en la forma en que ya hemos expuesto, analizando para ello, por un lado lo que denominaremos "obligaciones derivadas de la mera presencia en Internet", de una forma estática por completo y, por otro lado, lo que denominaremos "obligaciones de la entidad que realiza contratación electrónica", como referencia abierta a una presencia dinámica y conversacional.

a. Obligaciones derivadas de la mera presencia en Internet

Como ya hemos visto, existen diferentes maneras de estar presentes en Internet, y llevan distintas obligaciones aparejadas.

Las obligaciones de la mera presencia en Internet son generales, porque tener dicha presencia es indispensable para luego realizar cualquier otro tipo de acción. En definitiva, que las obligaciones resultan ser acumulativas, es decir, que quien realice contratación electrónica, además de cumplir las obligaciones generales, tiene que cumplir las específicas derivadas de dicha contratación.

Las entidades que tienen una mera presencia en Internet deben cumplir con las obligaciones previstas en la LCE para los prestadores de servicios en lo referente a lo siguiente:

a.1. Comunicar el nombre o nombres de dominio de Internet que le corresponda al Registro Público en el que conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad

Con el fin de garantizar que los ciudadanos y la Administración Pública le vinculen con su establecimiento físico y su "establecimiento" o localización en la red, cumpliendo el nombre de dominio una función de identificador comercial del prestador de servicios en la red, como examinaremos en un apartado posterior. A estos efectos el es-NIC, como entidad acreditada para el registro del dominio ".es", ha hecho público un modelo de comunicación [28] al Registro Mercantil para cumplir con esta obligación.

---

[27] La disposición adicional cuarta de la LCE sobre Modificación de los Códigos Civil y de Comercio modifica los artículos 1262 del Código Civil y 54 del Código de Comercio. En concreto, el artículo 1262 del Código Civil establece: "El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.

Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en el que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación".

El artículo 54 del Código de Comercio prevé: "Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en el que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación".

[28] Modelo que se encuentra disponible en la dirección de Internet del ES-NIC: https://www.nic.es/documentacion/lssi.html.

En el caso de los prestadores de servicios que ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberían haber solicitado la anotación de, al menos, uno de ellos en el registro público en el que figuren inscritos en el plazo de un año a contar desde la entrada en vigor de la LCE el 12 de octubre de 2002.

a.2. Proporcionar información, de manera permanente, fácil, directa y gratuita, sobre:

a. Nombre o denominación social.

b. Residencia o domicilio, o la dirección de uno de sus establecimientos permanentes en España.

c. Dirección de correo electrónico.

d. Otros datos que permitan establecer una comunicación directa y efectiva.

e. Datos de inscripción del nombre de dominio en el Registro en el que conste.

f. Si se somete a autorización administrativa, los datos relativos a la misma y del órgano de supervisión.

g. Si ejerce una profesión regulada, los datos que se refieran a la misma:

   1. Los datos del Colegio profesional al que, en su caso, pertenezca colegiado.

   2. El título académico oficial o profesional con el que cuente.

   3. El Estado de la Unión Europea o del Espacio Económico Europeo que expidió dicho título y, en su caso, la correspondiente homologación

   4. Las normas profesionales aplicables al ejercicio de su profesión a través de los cuales se puedan conocer, incluidos los electrónicos.

h. Número de identificación fiscal.

i. Precio del producto o servicio, indicando si se incluyen o no los impuestos y, en su caso, los gastos de envío.

j. Códigos de conducta a los que esté adherido, y la manera de consultarlos por vía electrónica.

Como veremos más detenidamente después, la LCE promueve el uso de instrumentos de autorregulación o códigos de conducta para que se adecuen los diversos preceptos de la Ley a las características específicas de cada sector.

Si se trata de un prestador de servicios de tarificación adicional, tendrá que proporcionar también la siguiente información:

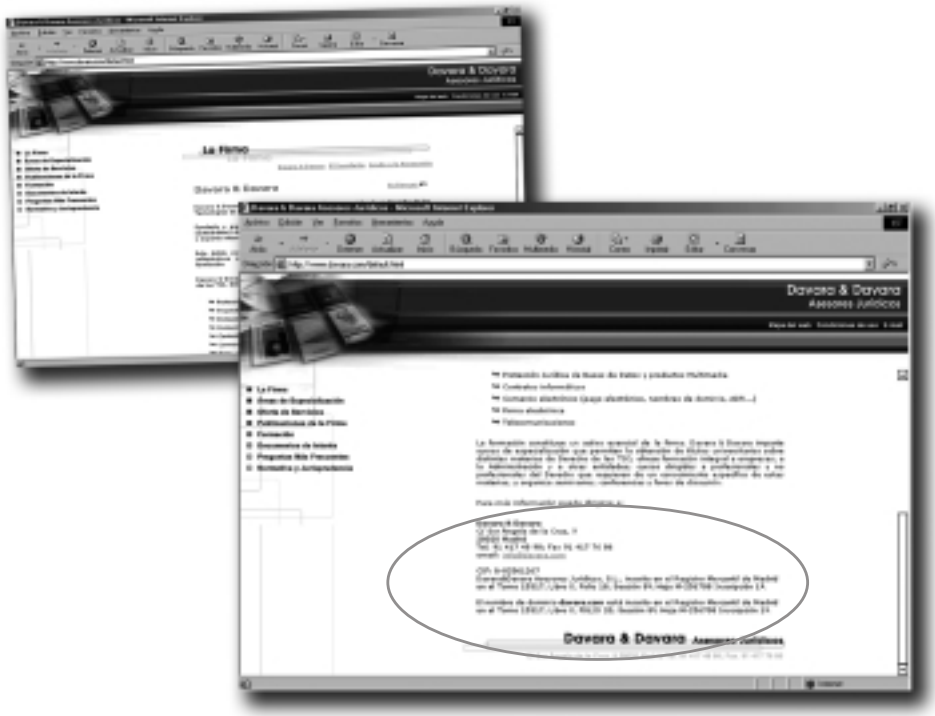
a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La obligación de proporcionar esta información se considera cumplida si el prestador la incluye en su página o sitio de Internet. En este sentido, a modo de ejemplo, se incluye la página de presentación de la Firma Davara & Davara, Asesores Jurídicos, en la dirección de Internet www.davara.com.



Como puede comprobarse, en la página de presentación de la Firma se incluye la información exigida por el artículo 10 de la LCE relativa a los siguientes aspectos:

- Denominación social: se indica Davara & Davara Asesores Jurídicos, S.L.
- Domicilio: se señala que el domicilio de la entidad es C/ Sor Ángela de la Cruz, 9, 28020 Madrid.
- Dirección de correo electrónico: info@davara.com
- Cualquier otro dato que permita establecer una comunicación directa y efectiva: en este caso se proporciona el número de teléfono 91 417 48 98 y el número de fax 91 417 76 86.
- Se proporcionan los datos de la inscripción de Davara & Davara Asesores Jurídicos, S.L. en el Registro Mercantil de Madrid.
- Se indican los datos de la inscripción del nombre de dominio <davara.com> en el Registro Mercantil de Madrid.
- Por último, se indica el número de identificación fiscal que corresponde a Davara & Davara Asesores Jurídicos, S.L.

a.3. Con arreglo al artículo 36 de la LCE todo prestador de servicios tiene la obligación de facilitar al Ministerio de Industria, Turismo y Comercio[29] y a los demás órganos previstos en la Ley la información y la colaboración precisas para el ejercicio de sus funciones.

Asimismo deberá permitir el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate por los agentes o el personal inspector de los órganos competentes.

[29]Aunque la LCE hablaba del Ministerio de Ciencia y Tecnología, que ya ha sido suprimido, dicha referencia tiene que entenderse hecha al Ministerio de Industria, Turismo y Comercio conforme al Real Decreto 553/2004, de 17 de abril, por el que se reestructuran los departamentos ministeriales, publicado en el Boletín Oficial del Estado número 94, de 18 de abril. En este sentido, las referencias que se hagan a lo largo del presente capítulo al Ministerio de Ciencia y Tecnología han de entenderse realizadas al Ministerio de Industria, Turismo y Comercio.

a.4. Comunicaciones comerciales por vía electrónica hay que tener en cuenta que su envío no está permitido, salvo que hayan sido previamente solicitadas o se haya obtenido el consentimiento previo de los destinatarios. Es necesario que las comunicaciones comerciales que se realicen por vía electrónica se identifiquen claramente como tales, incluyendo al principio del mensaje la palabra "publicidad", y que indiquen la persona física o jurídica en nombre de la cual se efectúan.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (en adelante, LGT) ha modificado este precepto introduciendo la posibilidad de utilizar direcciones de correo electrónico obtenidas lícitamente durante la contratación previa de bienes y servicios cuando sea para remitir publicidad de los bienes y servicios de su propia empresa que sean similares a los inicialmente contratados.

La LCE define las comunicaciones comerciales en el apartado f) de su Anexo como:

> *"Toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.*
>
> *A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica".*

En relación con las comunicaciones comerciales y las ofertas promocionales que se realicen por vía electrónica, además de regirse por la LCE, se tiene que observar la normativa prevista en materia comercial y de publicidad que se encuentre vigente.

Asimismo, cuando dichas comunicaciones comerciales vayan dirigidas a una persona física, se aplicará la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su correspondiente normativa de desarrollo, en especial, en todo lo referente a la obtención de los datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos de carácter personal.

La regulación jurídica que de las comunicaciones comerciales realiza la LCE ha sido modificada por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en particular, en lo que a las comunicaciones comerciales se refiere, en los artículos 21, 22, 38.3 b) y 38.4 d) de la LCE.

Con estas modificaciones, la regulación vigente obliga a que las comunicaciones comerciales que se efectúen por vía electrónica sean identificables claramente como tales y que se indique la persona física o jurídica en nombre de la cual se realizan. En el caso de que las comunicaciones comerciales se envíen a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra **"publicidad".**

Por su parte para el envío de **ofertas promocionales** tales como las que incluyan descuentos, premios y regalos, y de concursos o juegos, se deberá contar con autorización previa de su destinatario, se han de identificar claramente como tales e indicar la persona física o jurídica en nombre de la cual se realizan, y cumplirán con las normas de ordenación del comercio. Asimismo, las condiciones de acceso y, en su caso, de participación, deberán expresarse de manera clara e inequívoca.

Otro aspecto de las comunicaciones comerciales es que deben ser previamente solicitadas o expresamente autorizadas por sus destinatarios, la LCE prohíbe el envío de comunicaciones de carácter publicitario o promocional a través de correo electrónico o de otro medio de comunicación electrónica equivalente *si previamente no han sido solicitadas por sus destinatarios o expresamente autorizadas por los mismos.*

La modificación de la LGT ha introducido la posibilidad de utilizar aquellas direcciones de correo electrónico que habiéndose obtenido lícitamente durante la contratación previa de bienes y servicios se utilicen para remitir publicidad referente a bienes y servicios de su propia empresa que sean similares a los que ya fueron contratados por el cliente, con la obligación de ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito en el momento de la recogida de datos y en cada una de las comunicaciones comerciales que le dirija.

Hay que tener en cuenta que constituye infracción grave, sancionada con multa de 30.001 a 150.000 euros, el envío masivo de estas comunicaciones, por correo electrónico u otro medio de comunicación electrónica equivalente, a destinatarios que no las hayan autorizado o que no se hayan opuesto a ellas y, también, enviar más de tres comunicaciones por los medios anteriores, en el plazo de un año, a un mismo destinatario que no hubiera solicitado o autorizado dicha remisión o no se hubiese opuesto a ella.

El destinatario de las comunicaciones comerciales podrá revocar el consentimiento que otorgó para la recepción de comunicaciones comerciales. Para ello deberá notificar su voluntad al remitente de las comunicaciones comerciales. En este sentido, los prestadores de servicios deben procurar procedimientos sencillos y gratuitos con el fin de que los destinatarios que no quieran recibir más comunicaciones de este tipo puedan revocar el consentimiento que prestaron. La información sobre dichos procedimientos ha de estar accesible por medios electrónicos.

Todo lo anterior sin olvidar que, en el caso de que se traten datos de carácter personal, además de lo anterior deberá cumplirse también con todas las exigencias de la normativa específica.

COMUNICACIONES COMERCIALES POR VÍA ELECTRÓNICA

<table>
<tr><td rowspan="3">INFORMACIÓN EXIGIDA</td><td rowspan="2">COMUNICACIONES COMERCIALES</td><td>Por vía electrónica</td><td>Deberán:
– Ser claramente identificables como tales.
– Indicar la persona física o jurídica en nombre de la cual se realizan.</td></tr>
<tr><td>Por correo electrónico u otro medio de comunicación elect. equivalente</td><td>Además incluirán al comienzo del mensaje la palabra “publicidad”.</td></tr>
<tr><td>OFERTAS PROMOCIONALES Y CONCURSOS</td><td colspan="2">Deberán, previa autorización correspondiente:
– Ser claramente identificables como tales.
– Expresarse clara e inequívocamente las condiciones de acceso y participación.</td></tr>
<tr><td>PROHIBICIÓN</td><td colspan="3">Regla general: Enviar comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica, que no hubieran sido solicitadas con anterioridad o expresamente autorizadas por los destinatarios.
Excepción: En el caso de existir una relación contractual previa y de haber obtenido lícitamente los datos de contacto del cliente, se le pueden enviar comunicaciones comerciales referentes a productos o servicios similares a los que fueron objeto de contratación de su propia empresa, ofreciendo en todo caso la posibilidad de oponerse a las mismas.</td></tr>
<tr><td>DERECHOS DE LOS DESTINATARIOS</td><td colspan="3">– Revocar el consentimiento notificando su voluntad al remitente.
– A conocer electrónicamente información sobre los procedimientos de revocación del consentimiento, que deben habilitar los prestadores de servicios.</td></tr>
</table>

En la tabla que sigue a continuación se exponen, de manera resumida, las obligaciones mencionadas.

OBLIGACIONES GENERALES DE LOS PRESTADORES DE SERVICIOS	
Constancia registral del nombre de dominio	✓ En el Registro Mercantil o en otro Registro Público en el que figure ◆ Un nombre de dominio o dirección de Internet – En el plazo de 1 año desde la entrada en vigor de la LCE si ya vinieran usándolos ◆ Cualquier sustitución o cancelación de los mismos
Informar permanente, fácil, directa y gratuitamente	✓ Nombre o denominación social ✓ Domicilio o dirección del establecimiento permanente en España ✓ Dirección de correo electrónico ✓ Otros datos que permitan una comunicación directa y efectiva ✓ Datos de inscripción en el Registro Público en el que figuren ✓ Si su actividad se sujeta a autorización administrativa previa, los datos de dicha autorización y los identificativos del órgano encargado de supervisión ✓ Si ejerce una profesión regulada: ◆ Datos del Colegio Profesional y número de colegiado ◆ Título académico y su lugar de expedición ◆ Normas profesionales aplicables a su profesión ✓ El número de identificación fiscal ✓ Precio del producto o servicio, indicando si incluye impuestos y, en su caso, gastos de envío ✓ Códigos de conducta a los que esté adherido **En el caso de que se trate de prestadores de servicios de tarificación adicional informará de:** ✓ Características del servicio a proporcionar ✓ Funciones que efectuarán los programas informáticos que se descarguen, incluido el número de teléfono a marcar ✓ Procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá ✓ Procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional

b. Obligaciones de quien realiza contratación electrónica

En caso de que una entidad efectúe contratación por medios electrónicos deberá cumplir las obligaciones que hemos descrito para el caso de tener una función estática, o de mera presencia en Internet, y, además, las obligaciones que derivan propiamente de la contratación electrónica.

b.1. Obligaciones generales

El primer grupo de obligaciones, recordemos, estaba constituido por las de comunicar el nombre de dominio al Registro Mercantil o al registro en el que estuviese inscrito para la constitución de su personalidad jurídica o a los solos efectos de publicidad, y de unas cuantas obligaciones más que fundamentalmente tenían carácter informativo.

b.2. Obligaciones específicas

Para los prestadores de servicios que desarrollan una presencia dinámica contractual, además de cumplir con las obligaciones generales mencionadas, se acumulan una serie de obligaciones específicas.

- **Previas a la contratación**

En primer lugar la *obligación de informar con carácter previo* al inicio del procedimiento de contratación de los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

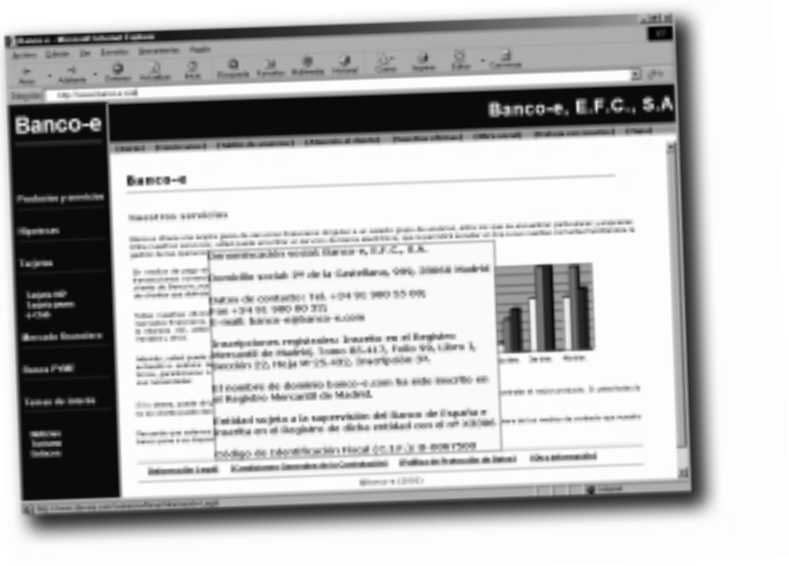
d) la lengua o lenguas en que podrá formalizarse el contrato.

Además deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Como excepción a esta obligación cuando ninguno de los contratantes tenga la condición de consumidor no se tendrá que facilitar esta información anterior siempre que así lo acuerden, o en caso de que el contrato se haya celebrado exclusivamente a través de correo electrónico u otro tipo de comunicación electrónica equivalente y siempre que no se usen estos medios con el fin de eludir dicha obligación de informar.

En cuanto al plazo de validez de las ofertas o propuestas de contratación que se efectúen por vía electrónica, éstas serán válidas durante el período que fije el oferente. Si el oferente no fija plazo alguno las ofertas serán válidas durante el tiempo que permanezcan accesibles a los destinatarios. Estos períodos de duración establecidos en la LCE se aplicarán sin perjuicio de lo previsto en la legislación específica.

En este caso, se presenta un ejemplo ficticio que permitirá ver cómo se cumplen las obligaciones en materia de información que se impone a un prestador de servicios que realiza contratación a través de Internet. En concreto, se ha creado el sitio web de una entidad financiera en la que se incluye la información que exige la LCE, tanto general como específica de la contratación de los bienes o productos que se ofrecen a través de este sitio web.



Por lo que se refiere a la información general que exige la LCE, a efectos de comprobar su cumplimiento práctico cabe señalar aquí que la información que se proporciona a través del apartado denominado "Información legal" es la siguiente:

- Denominación social: se indica Banco-e, E.F.C., S.A.
- Domicilio: en este apartado se indica cuál es la dirección del domicilio social de la entidad.
- Dirección de correo electrónico: se proporciona una dirección de correo electrónico de contacto.
- Cualquier otro dato que permita establecer una comunicación directa y efectiva: en este caso se proporciona un número de teléfono y un número de fax.
- Se proporcionan los datos de la inscripción de Banco-e en el Registro Mercantil correspondiente.
- Se indican los datos de la inscripción del nombre de dominio "banco-e.com" en el Registro Mercantil en el que la entidad está inscrita a efectos de su constitución.
- Por tratarse de una entidad financiera, se señala que es una entidad sujeta a la supervisión del Banco de España.
- Por último, se indica el código de identificación fiscal que corresponde a la entidad ficticia Banco-e, E.F.C., S.A.

En cuanto a la sujeción a Condiciones Generales de la Contratación (CGC) de los bienes o servicios proporcionados por esta entidad financiera, en el apartado denominado "Condiciones Generales de la Contratación" el consumidor accede a una pantalla en la que se presentan dichas condiciones generales, teniendo la posibilidad de imprimirlas y guardarlas, tal y como exige la LCE.

Además de esta información, en el caso de esta entidad ficticia el consumidor podría acceder a los apartados de "Política de Protección de Datos" a través del que se proporciona la información exigida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

- **Posteriores a la contratación efectuada**

En segundo lugar y una vez realizada la contratación, debe *confirmar a los destinatarios la recepción de la aceptación* a través de:

a. Un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente y en el plazo de veinticuatro horas siguientes a la recepción de la aceptación.

b. 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.

En los supuestos en que la obligación de confirmar la aceptación corresponda al destinatario de los productos o servicios, el prestador ha de facilitar el cumplimiento de esta obligación proporcionando al destinatario alguno de los medios citados anteriormente.

Se considera que se ha recibido la aceptación y su confirmación cuando las partes puedan tener constancia de ello. Pero en el caso de que la recepción de la aceptación se confirme mediante acuse de recibo se presume que el destinatario tiene constancia desde que el acuse se almacenó en el servidor correspondiente a su cuenta de correo electrónico o en el dispositivo utilizado para la recepción de comunicaciones.

Existen dos casos en los que no es necesario confirmar que se recibió la aceptación, por un lado, si ambos contratantes así lo acuerdan y ninguno tiene la consideración de consumidor o, por otro lado, si el contrato se celebró exclusivamente por intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, salvo que se lleve a cabo con el propósito de eludir el cumplimiento de la obligación de confirmar la recepción de la aceptación.

OBLIGACIONES GENERALES DE LOS PRESTADORES DE SERVICIOS[30]	
Constancia registral del nombre de dominio	✓ En el Registro Mercantil o en otro Registro Público en el que figure ◆ Un nombre de dominio o dirección de Internet – En el plazo de 1 año desde la entrada en vigor de la LCE si ya vinieran usándolos ◆ Cualquier sustitución o cancelación de los mismos
Informar permanente, fácil, directa y gratuitamente	✓ Nombre o denominación social ✓ Domicilio o dirección del establecimiento permanente en España ✓ Dirección de correo electrónico ✓ Otros datos que permitan una comunicación directa y efectiva ✓ Datos de inscripción en el Registro Público en el que figuren ✓ Si su actividad se sujeta a autorización administrativa previa, los datos de dicha autorización y los identificativos del órgano encargado de supervisión ✓ Si ejerce una profesión regulada: ◆ Datos del Colegio Profesional y número de colegiado ◆ Título académico y su lugar de expedición ◆ Normas profesionales aplicables a su profesión ✓ El número de identificación fiscal ✓ Precio del producto o servicio, indicando si incluye impuestos y, en su caso, gastos de envío ✓ Códigos de conducta a los que esté adherido

[30]Reproducimos de nuevo la tabla de obligaciones generales, aún a riesgo de resultar reiterativos, con el único fin de facilitar la lectura y evitar tener que volver a un apartado anterior, al tiempo que reiteramos la necesidad para estos prestadores de servicios de cumplir con todas las obligaciones mencionadas.

	En el caso de que se trate de prestadores de servicios de tarificación adicional informará de: ✓ Características del servicio a proporcionar ✓ Funciones que efectuarán los programas informáticos que se descarguen, incluido el número de teléfono a marcar ✓ Procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá ✓ Procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional

OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS QUE REALIZAN CONTRATACIÓN ELECTRÓNICA	
Información previa	Con carácter previo debe informar de los siguientes extremos: ✓ Los distintos trámites que deben seguirse para celebrar el contrato ✓ Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible ✓ Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos ✓ La lengua o lenguas en que podrá formalizarse el contrato ✓ Poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario
Información posterior	Confirmar la recepción de la aceptación mediante: ✓ Un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente y en el plazo de veinticuatro horas siguientes a la recepción de la aceptación ✓ 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

b.3. Obligaciones específicas de los prestadores de servicios de intermediación

Además de las obligaciones que la LCE impone a los prestadores de servicios, tanto generales como específicas en función de la actividad que desarrollen a través de Internet, dado que los prestadores de servicios de intermediación prestan determinados Servicios de la Sociedad de la Información a los que ya hemos hecho referencia, como por ejemplo los buscadores, etc., la Ley ha previsto que éstos tengan que cumplir además con otras obligaciones en virtud del desarrollo de su actividad y que son, de un lado, el deber de colaboración con los órganos competentes y, de otro lado, el deber de retención de los datos de tráfico.

- El deber de colaboración

Este deber específico de colaboración debe entenderse con independencia del deber de colaboración que la Ley impone a todos los prestadores de servicios (art. 36 de la LCE). En concreto, supone que los prestadores de servicios de intermediación tengan que cumplir las órdenes que sean dadas por un órgano competente con el fin de interrumpir la prestación de un Servicio de la Sociedad de la Información o de retirar determinados contenidos que provengan de prestadores de servicios establecidos en España, procediendo en su caso a suspender la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de otro servicio de intermediación que lleven a cabo.

En la adopción de dichas medidas se deberá atender a las garantías y procedimientos establecidos en el ordenamiento jurídico con el fin de no vulnerar los derechos a la intimidad personal y familiar, la protección de datos personales o la libertad de expresión y la libertad de información, cuando éstos pudieran verse afectados por la adopción de las mismas. Por último, estas medidas tendrán que ser objetivas, proporcionadas y no discriminatorias.

- **El deber de retención de los datos de tráfico**

Esta obligación, cuyo desarrollo reglamentario todavía está pendiente, al igual que muchos otros aspectos contenidos en la LCE, implica que los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones electrónicas que se establezcan para la prestación de un Servicio de la Sociedad de la Información.

Los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de redes de telecomunicaciones retendrán únicamente los datos necesarios para facilitar la localización del equipo terminal utilizado. Por su parte, los prestadores de servicios de alojamiento de datos retendrán los datos que sean imprescindibles para identificar el origen de los datos alojados y el momento en el que se inició la prestación del servicio.

En la retención de estos datos, que podrá ser por un período máximo de doce meses como prevé la LCE, los prestadores de servicios de intermediación tienen que garantizar las medidas de seguridad que eviten su pérdida, alteración o acceso no autorizado. Los datos así retenidos quedarán a disposición de los Jueces o Tribunales o del Ministerio Fiscal que podrían solicitarlos en el marco de una investigación criminal o para otros fines de seguridad pública o de defensa nacional. Cuando los datos vayan a ser comunicados a las Fuerzas y Cuerpos de Seguridad se deberá atender a lo establecido en la LOPD.

9. CONDICIONES GENERALES DE LA CONTRATACIÓN

El artículo 1.1 de la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación (LCGC)[31] define éstas como aquellas cláusulas que han sido incorporadas al contrato por imposición de una de las partes, indicando que

> *"Son condiciones generales de la contratación las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos".*

Como ya hemos dicho, el cumplimiento de la LCE no exime del cumplimiento de la normativa específica, que en el caso de las CGC se encuentra recogida en el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con Condiciones Generales de la Contratación, en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación.

Por lo tanto, además de las referencias que al uso de las CGC en la contratación electrónica puedan existir en la LCE (por ejemplo art. 27.4), hay que remitirnos al estudio de esta norma, si bien tenemos que avisar que la Disposición Final quinta de la LCE[32] anuncia que este Real Decreto tendrá que ser

[31] *Publicada en el Boletín Oficial del Estado núm. 89, de 14 de abril.*

[32] *"Disposición final quinta. Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales a esta Ley.*

El Gobierno, en el plazo de un año, modificará el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, para adaptar su contenido a lo dispuesto en esta Ley.

En dicha modificación, el Gobierno tendrá especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, conforme al mandato recogido en el artículo 9.1 de la Directiva 2000/31/CE".

modificado para adaptarse a la LCE teniendo especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, por lo que a lo mejor la obligación de remitir el texto puede suponer un obstáculo sobre todo si se piensa en nuevos medios, como la utilización de teléfonos móviles, en los que el soporte no parece el más adecuado, y debe pensarse en la puesta a disposición del usuario de las CGC más que en la remisión.

El objeto de este Real Decreto es regular la contratación a distancia con condiciones generales entre un empresario o profesional y un consumidor.

En cuanto a las obligaciones de los prestadores de servicios en Internet que utilicen CGC, hay que diferenciar dos momentos en los que el prestador ha de cumplir determinadas obligaciones:

1. *Con anterioridad a la celebración del contrato, el prestador de servicios:*

   - ha de informar a los posibles consumidores de todas las cláusulas del contrato, como mínimo en los tres días naturales anteriores a la contratación;
   - deberá remitir, por cualquier medio adecuado a la técnica de comunicación a distancia el texto íntegro de las condiciones generales que regulan la contratación en cuestión.

Por su parte el art. 27 de la LCE dispone en su apartado 4:

> *"Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario".*

2. *Con posterioridad a la celebración del contrato, el prestador de servicios:*

   - debe enviar la justificación de la contratación que se ha efectuado por escrito o en cualquier otro soporte duradero que sea adecuado al medio de comunicación empleado. Tal justificación debe contener la información, con todos sus términos, relacionada con la contratación que se ha llevado a cabo. El plazo máximo establecido para este envío es el momento de entrega de la cosa o el comienzo de la ejecución del contrato.

Con respecto a otras cuestiones acerca de las Condiciones Generales de la Contratación hay que destacar la existencia de un Registro de Condiciones Generales de la Contratación[33] cuya finalidad es la inscripción declarativa de cláusulas contractuales y de sentencias sobre las mismas con el objetivo de dar publicidad a su contenido y, así, proteger a los consumidores de la utilización de cláusulas abusivas y permitir el ejercicio de las acciones contra aquéllas que no se ajusten a los requisitos establecidos legalmente.

Hay que tener en cuenta, como ya hemos dicho, que el Gobierno tiene la obligación de facilitar la utilización de los contratos electrónicos y, por este motivo, con la entrada en vigor de la LCE, disponía de un plazo de un año para adaptar el contenido de la regulación sobre contratación telefónica o electrónica con condiciones generales a lo dispuesto en la LCE.

[33] *Aprobado por el Real Decreto 1828/1999, de 3 de diciembre, por el que se aprueba el Reglamento del Registro de Condiciones Generales de la Contratación, publicado en el Boletín Oficial del Estado núm. 306, de 23 de diciembre.*

10. CÓDIGOS DE CONDUCTA, ACCIÓN DE CESACIÓN Y ADR

a. Códigos de conducta

Los códigos de conducta, también denominados códigos tipo, éticos o deontológicos, son *un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector* según establece el apartado IV de la Exposición de Motivos de la LCE.

Los códigos tipo no son normas legales sino que tienen carácter de códigos deontológicos o de buena práctica profesional, además, son voluntarios y las partes deciden libremente su adhesión a los mismos. La función esencial de los códigos de conducta consiste en adecuar las disposiciones de la Ley a las actividades propias de cada sector.

El artículo 18 de la LCE prevé el posible contenido de los códigos de conducta y así:

> *"Podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información".*

En el ámbito de las materias reguladas por la LCE, las Administraciones Públicas están llamadas a impulsar la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores. Para el ámbito comunitario o internacional será la Administración General del Estado la que fomente su elaboración.

Cuando el contenido de los códigos de conducta afecte a sus respectivos intereses se garantizará la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas en la elaboración de los mismos. Asimismo, se tendrá especial consideración con relación a la protección de los menores y a la dignidad humana cuando el contenido del código de conducta les afecte y, en caso necesario, podrán desarrollarse códigos específicos sobre estas materias.

La LCE dispone que los códigos de conducta han de ser accesibles electrónicamente y que con la finalidad de darles mayor difusión se fomentará su traducción a otras lenguas oficiales en la Comunidad Europea.

A partir de la entrada en vigor de la LCE el Gobierno disponía del plazo de un año para aprobar un distintivo que permita identificar a los prestadores de servicios que respeten los códigos de conducta que se adopten con la participación del Consejo de Consumidores y Usuarios y que incluyan la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos.

En este sentido, se aprobó el Real Decreto 292/2004[34], de 20 de febrero, por el que se crea el distintivo público de confianza en los Servicios de la Sociedad de la Información y de Comercio Electrónico y se regulan los requisitos y procedimiento de concesión. Este Real Decreto 292/2004 tiene por objeto crear el distintivo que podrán mostrar los prestadores de servicios que se adhieran a códigos de conducta siempre y cuando cumplan con las condiciones previstas en el capítulo II del mismo.

El distintivo creado a través del Real Decreto 292/2004 se denomina «distintivo público de confianza en línea» y su formato es el siguiente:

[34] *B.O.E. núm. 50, de 27 de febrero de 2004.*

Este Real Decreto establece las condiciones que deben reunir los códigos de conducta, la concesión y retirada del distintivo y el procedimiento aplicable. En general, los requisitos de los códigos de conducta son los siguientes:

- Deberán estar redactados en términos claros y accesibles.
- Deben respetar la legalidad vigente e incluir, como mínimo, con suficiente grado de precisión:
  - ◆ Las garantías concretas que ofrecen a los consumidores y usuarios que mejoren o incrementen las reconocidas por el ordenamiento jurídico.
  - ◆ Un sistema de resolución extrajudicial de conflictos.
  - ◆ Los compromisos específicos que asumen los prestadores de servicios adheridos en relación con los problemas concretos planteados a los consumidores y usuarios del sector.
  - ◆ El ámbito de las actividades del prestador de servicios sometidas al código.
- Deberán contemplar la posibilidad de adhesión al código de prestadores de servicios que no sean miembros de la entidad promotora, siempre que la actividad desarrollada por éstos esté incluida en el ámbito del código.
- Deberá darse participación al Consejo de Consumidores y Usuarios.
- Deberán establecer, como medio de solución de controversias el sistema arbitral de consumo u otro sistema de resolución extrajudicial de conflictos:
  - ◆ Podrá hacerse uso de medios electrónicos.
- Deberán incluir procedimientos de evaluación independientes para comprobar el cumplimiento de las obligaciones asumidas por los prestadores de servicios adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

b. Solución judicial de conflictos: Acción de cesación

Uno de los aspectos fundamentales para impulsar la confianza de los consumidores en el comercio electrónico es la protección de los mismos a través del establecimiento de sistemas de resolución de conflictos frente a las conductas que resulten contrarias a la LCE y en los casos en que se lesionen intereses colectivos o difusos de los consumidores.

El Título V de la LCE, bajo la rúbrica *Solución judicial y extrajudicial de conflictos,* prevé dos tipos de solución de conflictos, el judicial y el extrajudicial. Dentro de la solución judicial se regula la interposición de la acción de cesación como consecuencia de la incorporación parcial a la LCE de la Directiva 98/27/CE del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores.

La acción de cesación se ejerce conforme a las prescripciones que, para esta clase de acciones, prevé la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Mediante el ejercicio de esta acción se podrá obtener una sentencia que:

- Condene al demandado a cesar la conducta contraria a la LCE y prohíba su reiteración futura.
- Prohíba la realización de una conducta aunque ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.

En virtud de lo previsto por la LCE, pueden interponer la acción de cesación por estar legitimados para ello activamente:

- Las personas físicas o jurídicas titulares de un derecho o interés legítimo.
- Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.
- Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, o, en su caso, en la legislación autonómica en materia de defensa de los consumidores.
- El Ministerio Fiscal.
- El Instituto Nacional de Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.
- Las entidades de otros Estados miembros de la Unión Europea constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el "Diario Oficial de las Comunidades Europeas.

c. La solución extrajudicial. Los medios alternativos de resolución de conflictos: ADR

c.1. Introducción

Los distintos sistemas de resolución extrajudicial de conflictos que existen conocidos como *ADR (Alternative Dispute Resolution)* los podemos clasificar en sistemas formales e informales. Entre los primeros están el Arbitraje, la Mediación y la Conciliación. Entre estos tres instrumentos no siempre existe una frontera clara, ni desde el punto de vista de su concepto ni menos desde el punto de vista de su aplicación práctica.

Por medio del Arbitraje, las personas en conflicto explican sus hechos, argumentos y pretensiones a un tercero y con ello éste decide en Derecho o en Equidad, según el caso, dando lugar normalmente a una resolución final y vinculante, aunque recurrible en otros casos.

En la Mediación, el mediador es un simple intermediario que pasa las propuestas de una y otra parte entre las dos, pero sin intervenir en las negociaciones, aunque suele registrar los acuerdos derivados de las mismas que además suelen tener valor contractual.

El conciliador participa activamente y sirve de guía para que las partes lleguen a un acuerdo. Si se llega a un acuerdo, éste se documenta en un contrato con fuerza entre las partes que lo suscriben.

Por su parte los sistemas de ADR informales son aquellos que median antes de que se produzca el conflicto, por ejemplo los servicios de atención al cliente o los "call centers". Los primeros son servicios internos ofertados por los vendedores, generalmente como un servicio de postventa que se presentan como una vía alternativa de resolución de conflictos distinta de los sistemas formales a los que nos acabamos de referir. Los "call centers" son un método de recepción y gestión de las reclamaciones de los consumidores que para ofrecer ciertas garantías deben cumplir unos requisitos de normalización y estandarización del proceso, es decir, debe existir un procedimiento más o menos uniforme que posibilite la satisfacción de los intereses del consumidor que recurre a ellos, proveyéndole de toda la información necesaria para cubrir sus reclamaciones, redirigiéndole a las instancias empresariales oportunas según el caso, de modo que sólo en caso de una discrepancia, y no de desatención, se encamine hacia un sistema de ADR o hacia un procedimiento judicial.

c.2. Impulso normativo a los sistemas de resolución extrajudicial de conflictos

Vistos los distintos sistemas de resolución extrajudicial de conflictos que existen, hay que destacar cómo en nuestro Ordenamiento Jurídico el impulso legal a la implantación de sistemas extrajudiciales de resolución de conflictos y en concreto al arbitraje, encuentra su pilar fundamental en el mandato constitucional del artículo 51 que insta a los poderes públicos a garantizar la defensa de los consumidores y usuarios mediante procedimientos eficaces, salvaguardando la seguridad, la salud y los legítimos intereses de los mismos. En este sentido, el art. 31 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios dispone que el Gobierno debía establecer un sistema arbitral sin formalidades especiales y cuyo sometimiento al mismo fuera voluntario, con el fin de que se solucionaran las quejas de los consumidores y usuarios, con carácter vinculante y ejecutivo para las partes interesadas. La entrada en vigor de la Ley 36/1988, de 5 de diciembre, de Arbitraje, supuso un nuevo impulso para el arbitraje de consumo y también decisivo puesto que encomendaba la regulación del procedimiento arbitral de consumo y, en su virtud, se promulgó el Real Decreto 636/1993, de 3 de mayo, que regula el Sistema Arbitral de Consumo. Actualmente se encuentra vigente la Ley 60/2003, de 23 de diciembre, de Arbitraje[35], que ha derogado a la Ley 36/1998.

Mediante la adhesión del prestador y del destinatario de los servicios al Sistema Arbitral de Consumo, la Junta Arbitral Nacional de Consumo u otras de ámbito inferior que estén autorizadas por el Instituto Nacional de Consumo, podrán resolver las disputas que planteen los consumidores de acuerdo con lo dispuesto en el Real Decreto 636/1993.

c.3. Sistema Arbitral de Consumo

En el Sistema Arbitral de Consumo el procedimiento se comienza a instancias del consumidor, siendo éste el que toma la iniciativa con una reclamación que identifique una cuestión determinada sobre las relaciones que haya tenido con un empresario o un comerciante. Es, por tanto, un sistema en el que el consumidor realiza una queja o reclamación respecto a una relación habida con un comerciante.

Este sistema no permite que todas las cuestiones sean objeto de arbitraje indicando que no podrán ser sometidos al mismo aquéllas en las que ya exista una sentencia judicial firme, salvo los aspectos derivados de su ejecución, las que traten sobre materias inseparablemente unidas a otras sobre las que las partes intervinientes no tengan capacidad de disposición, las que, de acuerdo con la normativa vigente, debe ser parte en el procedimiento el Ministerio Fiscal, en representación y defensa de quienes, por carecer de capacidad de obrar o de representación legal, no puedan actuar por sí mismos, o aquéllas en las que existan indicios racionales de haberse producido un delito o que concurran intoxicación, lesión o muerte.

La solicitud de arbitraje, que el consumidor presentará personalmente o a través de asociaciones de consumidores y usuarios, se podrá presentar por escrito o por medios electrónicos, informáticos y telemáticos.

Aunque las partes no tomen iniciativa alguna se continuará hasta el final ya que la inactividad de las partes no impide que se dicte el laudo que tendrá la misma eficacia y validez que si hubieran actuado activamente.

El laudo arbitral, que deberá dictarse en el plazo máximo de cuatro meses desde la designación del colegio arbitral, plazo que no podrá ser ampliado nada más que por acuerdo expreso de las partes, se expresará por escrito, con publicidad del lugar y fecha y de los nombres de los árbitros, debiendo estar argumentado y motivado cuando el colegio arbitral haya decidido la cuestión litigiosa conforme a derecho. El laudo será vinculante y producirá los efectos de “cosa juzgada”.

[35] *Publicada en el Boletín Oficial del Estado núm. 309, de 26 de diciembre.*

En consecuencia, el prestador y el destinatario de los servicios podrán someter sus conflictos a los arbitrajes establecidos en la legislación de arbitraje y de defensa de los consumidores y usuarios o a los procedimientos de resolución extrajudicial de conflictos *(ADR)* establecidos a través de los códigos de conducta o cualquier otro instrumento de autorregulación.

En los procedimientos para la resolución extrajudicial de conflictos pueden utilizarse medios electrónicos *(ODR, Online Dispute Resolution).* Los sistemas de ODR son sistemas de resolución de conflictos que se desenvuelven principalmente a través de Internet y deben ser tenidos en cuenta, por los prestadores que desarrollen su actividad por este medio puesto que constituyen un elemento fundamental para fomentar la confianza de quienes contraten sus bienes o servicios. En este sentido, debemos atender al Sistema de Información sobre Tramitación Arbitral (SITAR)[36] puesto en marcha por el Ministerio de Sanidad y Consumo, y que permite llevar a cabo el procedimiento de arbitraje de consumo a través de Internet para reclamaciones tanto de comercio físico como de comercio electrónico.

c.4. El arbitraje en el comercio electrónico

La LCE potencia la vía de la solución extrajudicial de conflictos, en concreto el recurso al arbitraje y a los procedimientos alternativos de resolución de controversias con el fin de dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás Servicios de la Sociedad de la Información.

Los beneficios que pueden suponer los mecanismos de resolución extrajudicial de conflictos, en especial del arbitraje en el comercio electrónico, serían los siguientes:

- *Accesibilidad:* el arbitraje ha de ser fácilmente accesible para las partes, evitando las cargas y los trámites burocráticos innecesarios.
- *Conveniencia:* puesto que el arbitraje se adecua a la controversia.
- *Rapidez:* el arbitraje debe representar un ahorro sustancial en tiempo frente al proceso jurisdiccional.
- *Resoluciones específicas, creativas y adaptadas al caso:* la especialización de los árbitros proporciona a las soluciones la posibilidad de su aplicación en la práctica.
- *Bajo coste:* el arbitraje ha de ser más asequible que su paralelo en la vía judicial, sobre todo desde el punto de vista económico y en el entorno de la contratación electrónica, donde las reclamaciones son numerosas pero de baja cuantía.
- *Trazabilidad y seguimiento:* las partes deben tener la posibilidad real de conocer la fase en la que se encuentra la controversia, los elementos probatorios presentados, los hechos que se han alegado, etc.
- *Reducción de la carga de trabajo de los mecanismos jurisdiccionales tradicionales:* la reconducción de los asuntos que colapsan el sistema judicial a otros sistemas especializados en resolver cuestiones específicas contribuirá a la mejora del funcionamiento del sistema judicial en conjunto.

[36] *Al que puede accederse en la dirección de Internet http://sitar.msc.es.*

11. RÉGIMEN DE RESPONSABILIDAD

Con carácter general los Prestadores de Servicios de la Sociedad de la Información están sujetos a la responsabilidad civil, penal y administrativa prevista en el ordenamiento jurídico. Pero, además, la LCE prevé un régimen de responsabilidad para los prestadores de servicios de intermediación que faciliten el acceso a redes de telecomunicaciones, transmitan datos a través de las mismas, realicen copia temporal de los datos que soliciten los usuarios, suministren servicios de alojamiento o almacenamiento de datos y que faciliten enlaces a contenidos o instrumentos de búsqueda.

Diferenciando el régimen de responsabilidad que corresponde a los prestadores de servicios en el ejercicio de actividades de intermediación, distinguiremos entre los que faciliten el acceso a una red de telecomunicaciones o transmitan los datos suministrados por el destinatario del servicio a través de la misma, los que realizan copia temporal de los datos que solicitan los usuarios, los que suministran servicios de alojamiento o almacenamiento de datos que le proporcionan los destinatarios o los que faciliten enlaces a contenidos o instrumentos de búsqueda.

a. Operadores de redes y proveedores de acceso

En cuanto a los prestadores de servicios de intermediación que faciliten el acceso a una red de telecomunicaciones o transmitan los datos suministrados por el destinatario del servicio a través de la misma no serán responsables de la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos. No se va a considerar modificación la manipulación técnica de los archivos que contienen los datos durante su transmisión.

b. Prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios

Aquellos prestadores de servicios de intermediación que realizan copia temporal de los datos que solicitan los usuarios (es decir, los almacenan en sus sistemas de forma automática, provisional y temporal para hacer más eficaz su transmisión ulterior a otros destinatarios) no serán responsables del contenido de esos datos ni por la reproducción temporal de los mismos siempre que cumplan las condiciones establecidas en la LCE, es decir, siempre que:

a) *No modifiquen la información.*

b) *Permitan el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.*

c) *Respeten las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.*

d) *No interfieran en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y*

e) *Retiren la información que hayan almacenado o hagan imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:*

   1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.

   2.º Que se ha imposibilitado el acceso a ella, o

   3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

c. Prestador de servicios de alojamiento o almacenamiento de datos

Los prestadores que suministran servicios de alojamiento o almacenamiento de datos que les proporcionan los destinatarios no serán responsables por la información almacenada cuando no tengan conocimiento efectivo de que es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización; o, si tiene conocimiento de todo ello, retira los datos o impide el acceso a los mismos. Esta exención de responsabilidad no operará en el caso de que el destinatario de la información esté actuando bajo la dirección, autoridad o control de su prestador de servicios de intermediación.

En este sentido, se entenderá que el prestador de servicios de intermediación tiene conocimiento efectivo de la ilicitud de la información o de que lesiona bienes y derechos de terceros cuando un órgano competente haya declarado efectivamente la ilicitud de los datos, su retirada, que se imposibilite el acceso a los mismos o la existencia de lesión, y el prestador conociera la correspondiente resolución.

d. Prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda

Respecto a los Prestadores de Servicios de la Sociedad de la Información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos, no van a ser responsables de la información a la que dirijan a los usuarios de sus servicios siempre y cuando no tengan conocimiento efectivo de que la información a la que remiten es ilícita o lesiona bienes o derechos de un tercero que son susceptibles de indemnización, o en el caso de que tenga conocimiento efectivo de todo esto, el prestador actúe diligentemente suprimiendo o inutilizando el correspondiente enlace. Esta exención de responsabilidad no se aplicará en el supuesto de que el destinatario de la información esté actuando bajo la dirección, autoridad o control de su prestador de servicios.

Así, se entenderá que el prestador tiene conocimiento de la ilicitud de la información o de que lesiona bienes y derechos si conoce la resolución dictada por un órgano competente que declare la existencia de lesión, la ilicitud de la información, ordenando su retirada o que se imposibilite el acceso a la misma.

12. INFORMACIÓN Y CONTROL

El Ministerio de Industria, Turismo y Comercio, órgano competente en materia de Telecomunicaciones y Sociedad de la Información y entre ellas ésta de comercio electrónico, tiene encomendadas, entre sus funciones, dos que debemos destacar en este punto, de un lado la de prestar, junto con otros órganos competentes, información relacionada con la materia de comercio electrónico y de otro lado, tiene asignada la función de supervisar y controlar la actividad de los prestadores de servicios.

a. Información

En relación con la primera función el Ministerio de Industria, Turismo y Comercio, así como los Ministerios de Justicia, Economía y Hacienda[37] y de Sanidad y Consumo, y los órganos que determinen las Comunidades Autónomas y Entidades Locales, están obligados a facilitar a los prestadores de servicios y a los destinatarios la información sobre sus derechos y obligaciones contractuales en el ámbito de la contratación electrónica, los procedimientos de resolución de los conflictos y las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La solicitud de esta información puede realizarse electrónicamente.

[37] *En virtud de la reestructuración efectuada por el Real Decreto 553/2004, de 17 de abril, por el que se reestructuran los departamentos ministeriales.*

Asimismo, el Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso a cualquier interesado a la información que haya recibido respecto de los órganos arbitrales y de los responsables de los demás procedimientos de resolución extrajudicial de conflictos.

En este sentido, el Consejo General del Poder Judicial enviará todas las resoluciones judiciales relevantes acerca de la validez y eficacia de los contratos celebrados electrónicamente, su utilización como prueba en juicio o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y prestadores. Y los órganos de resolución extrajudicial de los conflictos comunicarán aquellos laudos o decisiones que revistan importancia para la prestación de Servicios de la Sociedad de la Información y de Comercio Electrónico.

b. Control

El cumplimiento por los prestadores de servicios de las obligaciones previstas en la LCE y en las disposiciones que la desarrollen se controlará por el Ministerio de Industria, Turismo y Comercio, salvo en aquellas materias en las que órganos de carácter administrativo o jurisdiccionales sean competentes (por ejemplo, la Agencia Española de Protección de Datos respecto de tratamiento de datos de carácter personal, muy especialmente en las comunicaciones comerciales y más después de la Ley 32/2003, de 3 de noviembre General de Telecomunicaciones).

El ejercicio de esta función de control que tiene atribuida el Ministerio de Industria, Turismo y Comercio conlleva la realización de las actuaciones inspectoras que sean precisas. Los funcionarios que lleven a cabo la inspección tendrán la consideración de autoridad pública en el desempeño de sus funciones.

En relación con la actividad de control de los Servicios de la Sociedad de la Información, los prestadores de servicios tienen la obligación de facilitar al Ministerio de Industria, Turismo y Comercio toda la información y colaboración que sea necesaria para el ejercicio de sus funciones y, asimismo, permitirán a los agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación que resulte relevante para la actividad de control de que se trate.

13. INFRACCIONES Y SANCIONES

El Título VII de la LCE, bajo el epígrafe de *Infracciones y sanciones,* regula (arts. 37 a 45), un régimen sancionador al que estarán sometidos los Prestadores de Servicios de la Sociedad de la Información y en el que se califican las infracciones como leves, graves y muy graves (art. 38), estableciéndose multas que llegan hasta los 600.000 euros, graduándose la cuantía atendiendo a (art. 40):

a) La existencia de intencionalidad.

b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.

c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.

d) La naturaleza y cuantía de los perjuicios causados.

e) Los beneficios obtenidos por la infracción.

f) El volumen de facturación a que afecte la infracción cometida.

Las infracciones prescribirán a los tres años las muy graves, a los dos las graves y a los seis meses las leves y, con relación a las sanciones, también se establece un plazo de prescripción siendo de tres años para las que hayan sido impuestas como consecuencia de faltas muy graves, de dos años las consecuentes de faltas graves y de un año las que provengan de faltas leves.

En los procedimientos sancionadores por infracciones muy graves o graves se podrán acordar medidas de carácter provisional tales como:

a) La suspensión temporal de la actividad del prestador de servicios y, en su caso, el cierre provisional de sus establecimientos;

b) El precinto, depósito o incautación de registros, soportes, archivos, documentos, aparatos y equipos informáticos;

c) Advertir al público de la existencia de posibles conductas infractoras, de la incoación del expediente sancionador de que se trate y de las medidas adoptadas para el cese de dichas conductas.

En el caso de que las medidas provisionales acordadas no se cumplan, el órgano administrativo competente podrá imponer multas que no excederán de 6.000 euros por cada día sin cumplir.

La imposición de las sanciones por el incumplimiento de lo previsto en la LCE corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Turismo y Comercio, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información. Cuando se trate de infracciones que versen sobre comunicaciones comerciales remitidas a través de correo electrónico u otro medio de comunicación electrónica equivalente, la competencia sancionadora corresponde a la Agencia Española de Protección de Datos.

La siguiente tabla muestra el catálogo de infracciones previsto en la LCE con las sanciones que llevan aparejadas.

INFRACCIONES	SANCIONES
LEVES	
✓ La falta de comunicación al registro público en que estén inscritos del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información. ✓ No informar sobre: ◆ los datos de inscripción del nombre de dominio o dirección de Internet en el Registro correspondiente; ◆ los datos de la autorización administrativa y del órgano de control, si su actividad está sujeta a un régimen de autorización administrativa previa; ◆ si ejerce una profesión regulada: • los datos del Colegio Profesional al que pertenezca y el número de colegiado, • su título académico o profesional, • el Estado de la Unión Europea o del Espacio Económico Europeo en que se expidió el título y su homologación o reconocimiento, • las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los que se puede conocer. ◆ el número de identificación fiscal; ◆ los códigos de conducta a los que esté adherido y la manera de consultarlos electrónicamente. ✓ El incumplimiento de las obligaciones de información sobre las comunicaciones comerciales, ofertas promocionales y concursos. ✓ El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos para ello y no constituya infracción grave. ✓ No facilitar la información previa al procedimiento de contratación, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor. ✓ El incumplimiento de la obligación de confirmar la recepción de una petición, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.	HASTA 30.000 €

INFRACCIONES	SANCIONES
LEVES	
✓ El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos cuando empleen dispositivos de almacenamiento y recuperación de datos, cuando no constituya una infracción grave. ✓ El incumplimiento de la obligación del prestador de servicios de establecer procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave. ✓ El incumplimiento de la información por los prestadores de servicios de tarificación adicional cuando no constituya infracción grave.	HASTA 30.000 €
GRAVES	
✓ El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un Servicio de la Sociedad de la Información, salvo que deba ser considerado como infracción muy grave. ✓ El incumplimiento significativo de no proporcionar información sobre: ◆ su nombre o denominación social; residencia o domicilio o 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; ◆ el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, los gastos de envío. ✓ El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos para poder enviarlas. ✓ El incumplimiento significativo de la obligación del prestador de servicios en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios. ✓ No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en la Ley. ✓ El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor. ✓ La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley. ✓ El incumplimiento significativo de la obligación de proporcionar información por los prestadores de servicios de tarificación adicional. ✓ El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos cuando se utilicen dispositivos de almacenamiento y recuperación, de datos.	DESDE 30.001 € HASTA 150.000 €
MUY GRAVES	
✓ El incumplimiento de: ◆ las órdenes dictadas en virtud del artículo 8 de la Ley en aquellos supuestos en que hayan sido dictadas por un órgano administrativo; ◆ la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11 de la Ley. ✓ El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12 de la Ley. ✓ La utilización de los datos retenidos, en cumplimiento del deber de retención de los datos de tráfico, para fines distintos de los señalados en él.	DESDE 150.001 € HASTA 600.000 €

capítulo segundo

Seguridad en las transacciones electrónicas

1. FIRMA ELECTRÓNICA

El desarrollo de la Sociedad de la Información necesita de un ámbito generalizado de confianza en las comunicaciones telemáticas o electrónicas que poco a poco se va fraguando pero que requiere de impulsos como la aprobación de la Ley 59/2003, de 19 de diciembre, de firma electrónica[38] (en adelante, LFE).

1.1. Introducción

La firma electrónica es un instrumento que permite garantizar la autenticación del mensaje y de las partes, la integridad del mismo, esto es, que no ha sufrido variaciones desde que fue enviado por el remitente hasta que llega al destinatario. Del mismo modo por medio de la firma electrónica se evitan supuestos de repudio porque el remitente no puede alegar no haber enviado el mensaje. Además, también puede proporcionar confidencialidad.

Por estos caracteres la firma electrónica trata de llevar al entorno electrónico las mismas posibilidades que las firmas manuscritas ofrecen en el mundo *off line.* No toda firma electrónica tiene el mismo valor jurídico que las firmas manuscritas, deben reunir unos requisitos especiales para poder otorgar esta equivalencia funcional.

Conforme a la Ley de firma electrónica podemos distinguir tres tipos de firma electrónica, así, la firma electrónica que es *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*. En segundo lugar, la firma electrónica avanzada, que permite igualmente identificar al firmante y además detectar cualquier cambio ulterior de los datos firmados. Está vinculada al firmante de manera única y a los datos a que se refiere y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. En tercer y último lugar la firma electrónica reconocida que es la *firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*.

Visto esto decir que en el cuadro que representamos a continuación reflejamos como los tres tipos de firma tienen requisitos acumulativos que partiendo de la función de identificar al firmante van aportando al usuario nuevas funciones para que éste pueda optar por utilizar uno u otro tipo de firma según sus necesidades concretas en cada caso. Es importante interpretar el cuadro en el sentido de que las funciones de los tipos de firma se suman a las del tipo de firma anterior:

[38] *Publicada en el Boletín Oficial del Estado núm. 304, de 20 de diciembre.*

CLASES DE FIRMA ELECTRÓNICA	FUNCIONES
Firma electrónica	• Identificación del firmante.
Firma electrónica avanzada	• Detectar cualquier cambio ulterior de los datos firmados. • Vinculación al firmante y a los datos a que se refiere de manera única. • Creada por medios que el firmante puede mantener bajo su exclusivo control.
Firma electrónica reconocida	• Basada en un certificado reconocido. • Generada mediante un dispositivo seguro de creación de firma.

Con el fin de conocer mejor el funcionamiento de la firma electrónica es necesario atender a los conceptos de datos de creación de firma, dispositivo de creación de firma, dispositivo seguro de creación de firma y datos de verificación de firma. Así, la Ley entiende por datos de creación de firma *los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica*, por su parte un dispositivo de creación de firma se entiende como *un programa o sistema informático que sirve para aplicar los datos de creación de firma* y cuando este dispositivo tenga la consideración de seguro, que es el que se exige para que la firma electrónica tenga el carácter de reconocida, será porque además de reunir las características expuestas ofrezca al menos las siguientes garantías:

a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.*

b) *Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.*

c) *Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.*

d) *Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.*

Otros elementos que se deben conocer en el uso de la firma electrónica son los datos de verificación de firma electrónica que son *los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica* y por otro lado los dispositivos de verificación de firma electrónica que son los programas o sistemas informáticos que sirven para aplicar los datos de verificación de firma.

Por último, es necesario conocer que existen diferentes figuras que pueden intervenir en el funcionamiento de la firma electrónica, integrándose éstas en una Infraestructura de Clave Pública (PKI, *Public Key Infraestructure)* cuyo objeto es proporcionar servicios de certificación, entre los que se incluye la firma electrónica, a los usuarios. Así, y en orden jerárquico, encontramos en primer lugar la Autoridad Raíz, que es quien emite el certificado raíz en el que se basará la confianza del resto de certificados electrónicos que se emitan para las diferentes finalidades con las que se vayan a utilizar. Por debajo de esta Autoridad Raíz se encuentran las Autoridades de Certificación o Prestadores de Servicios de Certificación[39] (PSC), y las Autoridades de Registro, que se encargan de identificar a los solicitantes de certificados electrónicos, comprobando en su caso su identidad y remitiendo las correspondientes solicitudes a los PSC. Por último, encontramos a los usuarios de los servicios de certificación, que pueden ser titulares de un certificado electrónico y firmantes[40].

[39] *El artículo 2.2 de la LFE define al prestador de servicios de certificación como "la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica".*

[40] *El firmante es definido en el artículo 6.2 de la LFE 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".*

Dos son las características básicas que se deben tener en cuenta en el uso de la firma electrónica, de una parte, hay que establecer un método seguro para asociar una clave electrónica a una persona, de forma que, utilizándola, se pueda decir que está electrónicamente firmando el documento, y de otra parte, se necesitará otro método para poder comprobar, en el otro extremo, que es esa persona realmente la que firmó el documento.

Además, se busca garantizar que el documento viaja en un entorno seguro y no puede ser leído o modificado por un tercero no autorizado, aunque lo intercepte. Esto se consigue utilizando técnicas criptográficas con el objeto de cifrar los datos.

1.2. Criptografía

Los sistemas de cifrado más conocidos son dos y, muy someramente, podemos definirlos del siguiente modo:

- *Sistema de clave simétrica o secreta:* es aquél que está formado por una sola clave que sirve tanto para cifrar como para descifrar.
- *Sistema de clave asimétrica o pública*: en este caso existen asociadas a cada firmante de un documento dos claves diferentes, una de ellas sirve para cifrar y la otra para descifrar. Estas dos claves se denominan privada y pública, la primera cifra y con la segunda se descifra lo que se ha cifrado con la primera, y ninguna de ellas lleva a la otra. Esto es, se firma con la clave privada y se descifra la firma con la clave pública[41].

La clave privada permanece secreta y la clave pública se da a conocer para poder establecer el sistema completo. En la clave privada debe quedar garantizado que no se puede descubrir por lo que suelen emplear mayores longitudes de claves, teniendo en cuenta que un algoritmo de mayor longitud es más difícil de descubrir.

1.3. Validez y eficacia jurídica de la firma electrónica

Uno de los mayores frenos con los que se encuentra el instrumento de la firma electrónica es el de que al buscar trasladar la eficacia de la firma manuscrita al entorno electrónico se plantea la falta de reconocimiento del mismo valor jurídico.

La Ley de firma electrónica en su artículo 3 establece la equivalencia funcional de la firma electrónica reconocida con la manuscrita, no basta como establecía la anterior regulación de firma electrónica[42] con que se trate de una firma electrónica avanzada sino que además habrá de estar basada en un certificado reconocido y haber sido creada por un dispositivo seguro de creación de firma.

Todo esto sin perjuicio de los efectos jurídicos que deben reconocerse a una firma electrónica que no reúna los requisitos de firma electrónica reconocida con relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

1.4. Firma electrónica de personas jurídicas

Una de las novedades más importantes que introduce la Ley de firma electrónica es la de permitir la firma electrónica de las personas jurídicas integrándolas así en el tráfico telemático y yendo más allá del régimen anterior que sólo reconocía como firmantes a las personas físicas[43].

---

[41] El documento firmado con la clave privada de una persona, es entendido, o conocido quien es el firmante, descifrando con la clave pública de esa misma persona. Lo que se cifra con la clave privada se descifra con la clave pública.

[42] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

[43] "Art. 3. c) del Real Decreto-ley 14/1999: «Signatario»: Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.", mientras que el artículo 6.2 de la LFE dice que es firmante "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".

Éste es un caso distinto a la firma electrónica de los representantes de las personas jurídicas, supuesto ya habitual en la tradición jurídica, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados.

No obstante, conviene puntualizar que ya el artículo 5.3 del Real Decreto-Ley 14/1999 apuntaba esta posibilidad en el ámbito tributario, al decir: *3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-Ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica*. Esta redacción venía impulsada por el manifiesto éxito de la Administración electrónica tributaria en España, y parece que la Ley ha querido extender el ámbito de actuación, tal y como recalca en su Exposición de Motivos: *Se va así más allá del Real Decreto-Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.*

De un lado, como vemos, la figura parece complicada, puesto que siempre será una persona física quien pueda firmar, electrónica o manualmente, pues la firma implica una asunción de voluntad, y, de otro lado, se pretende inyectar un mayor dinamismo y eficiencia en las relaciones telemáticas de las empresas, huyendo del exigido formalismo y las cargas que la representación tradicional, en documento público, acarrea. En este sentido, la Exposición de Motivos de la Ley resalta en su apartado I que: *El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las Nuevas Tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas.*

En resumen, frente a la regulación del Real Decreto-Ley 14/1999, que en su artículo 3 definía al signatario únicamente como persona física, la Ley no sólo incluye la figura de la representación, sino que, además, introduce la muy novedosa figura de la firma de las personas jurídicas.

Uno de los problemas que más fácilmente se deducen del planteamiento de otorgar una firma a una persona jurídica, de la que, como decíamos, carece en el entorno tradicional obviamente, es el de la responsabilidad frente a terceros.

La Exposición de Motivos de la Ley, en este sentido, habla de varias cautelas: por un lado, dice que los solicitantes (evidentemente personas físicas) tienen que tener una legitimación especial, como se recoge en el artículo 7.1 [44], y, por otro, que se tendrán que responsabilizar de la custodia de los datos de creación de firma asociados a esos certificados, como dice el artículo 7.2 [45], además, de, finalmente, limita el uso de estos certificados a *los actos que integren la relación entre la persona jurídica y las Administraciones Públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse,* como señala el artículo 7.3 [46].

La expresión giro o tráfico ordinario pretende, según las palabras de la Exposición de Motivos de la Ley, adaptar a nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". No obstante, la misma Ley, consciente de la necesidad de concreción continúa intentando delimitar las actividades comprendidas en esta denominación: *se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las activida-*

[44] *Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.*

[45] *La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.*

[46] *Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.*

des de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. En definitiva, como ya apuntábamos, se trata de un supuesto más "cotidiano" y necesariamente menos formalista que el de la representación, máxime en un entorno como el electrónico que supuestamente necesita y busca eliminar las cargas burocráticas.

La misma Ley ya señala uno de los más evidentes puntos débiles de la cuestión, al decir que: *Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.*

Continuando con el razonamiento, el problema más inmediato surge, pues, con la responsabilidad frente a terceros de los actos realizados por estas personas físicas dependientes de la persona jurídica, que no son sus representantes en el sentido tradicional del ordenamiento jurídico, pero que, en definitiva, tienen capacidad para obligar a la persona jurídica a la que, en sentido coloquial y amplio de la palabra, representan.

En definitiva, se trata de un problema de límites y de definición, que consecuentemente conlleva un grado de inseguridad jurídica muy criticado por los detractores de esta nueva figura.

1.5. Certificados electrónicos

Un certificado electrónico es un documento electrónico que vincula una clave pública, es decir, los datos de verificación de firma, a una organización o particular. Viniendo así a permitir relacionar con toda seguridad un mensaje recibido con su remitente.

El sistema de emisión de certificados electrónicos por terceras partes de confianza es la solución técnica que se ha encontrado, a nivel europeo o comunitario y nacional, vinculando estos certificados de forma segura a unos datos de verificación de firma (una clave pública, en el caso de criptografía asimétrica) e indirectamente su correspondiente dato de creación de firma (clave privada) a una persona determinada.

La LFE distingue dos clases principales de certificados electrónicos: el certificado electrónico y el certificado electrónico reconocido diferenciándose uno de otro por los requisitos que se exigen en su emisión. Para conocer estos requisitos analicemos la tabla que sigue:

CLASES DE CERTIFICADOS ELECTRÓNICOS	REQUISITOS
Certificado electrónico	✓ Firmado electrónicamente por un prestador de servicios de certificación ✓ Vincula unos datos de verificación de firma a un firmante ✓ Confirma su identidad
Certificado reconocido	✓ Expedidos por un prestador de servicios de certificación que cumpla los requisitos de: ◆ Comprobar la identidad y circunstancias personales de los solicitantes de certificados ◆ Verificar que toda la información contenida en el certificado es exacta ◆ Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado ◆ Garantizar la complementariedad de los datos de creación y verificación de firma siempre que ambos sean generados por el prestador de servicios de certificación

El contenido que al menos deben incluir los certificados reconocidos se describe en artículo 11.2 de la Ley y los recogemos en la tabla que sigue a continuación:

CONTENIDO MÍNIMO DE LOS CERTIFICADOS RECONOCIDOS

1. La indicación de que se expiden como tales
2. El código identificativo único del certificado
3. Identificación, domicilio y firma electrónica avanzada del prestador de servicios de certificación
4. Identificación del signatario:
   a) Personas físicas:
      - ◆ Nombre, apellidos, DNI o
      - ◆ Seudónimo que conste como tal de manera inequívoca
   b) Persona jurídica:
      - ◆ Denominación social
      - ◆ Código de Identificación Fiscal
5. Datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante
6. Comienzo y el fin del período de validez del certificado
7. Los límites de uso del certificado, si se establecen
8. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen

La consignación en el certificado reconocido de cualquier otra información relativa al firmante se realizará cuando sea significativo en función del fin propio del certificado y siempre que el firmante lo solicite.

1.6. Prestadores de servicios de certificación

Los sujetos que intervienen en el sistema de firma electrónica son además de los firmantes, los prestadores de servicios de certificación que son los que emiten los certificados electrónicos o reconocidos que hemos analizado en el epígrafe anterior.

Los prestadores de servicios de certificación deben formular una Declaración de prácticas de certificación que estará disponible al público de manera fácilmente accesible al menos por vía electrónica y de forma gratuita. En esta Declaración se hará constar la información que exponemos en la tabla:

DECALARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Obligaciones relativas a la gestión de los datos de:
- ◆ Creación
- ◆ Verificación de firma
- ◆ Los certificados electrónicos

Las condiciones aplicables a:
- ◆ La solicitud
- ◆ Expedición
- ◆ Uso
- ◆ Suspensión
- ◆ Extinción
  - De la vigencia de los certificados

DECALARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (continuación)

- Las medidas de seguridad técnicas y organizativas
- Los perfiles
- Los mecanismos de información sobre la vigencia de los certificados

En su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos Registros.

Las obligaciones principales de los prestadores de servicios, partiendo de la base de que los prestadores de servicios que emitan certificados reconocidos deberán cumplir las obligaciones generales de los prestadores de servicios y además unas específicas que señala el artículo 20 de la Ley de firma electrónica, veamos gráficamente cuáles son estas obligaciones:

OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

OBLIGACIONES GENERALES	No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
	Información mínima al firmante, de forma gratuita, por escrito o por vía electrónica: ◆ Sus obligaciones. ◆ La forma en que han de custodiarse los datos de creación de firma. ◆ El procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de: • dichos datos y • determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido. ◆ Mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo. ◆ Método utilizado para comprobar la identidad del firmante u otros datos que figuren en el certificado. ◆ Condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial. ◆ Certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad. ◆ Demás informaciones contenidas en la declaración de prácticas de certificación.
	Mantener un Directorio actualizado de certificados que expidan.
	Servicio de consulta sobre la vigencia de los certificados rápido y seguro.
OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN QUE EMITAN CERTIFICADOS RECONOCIDOS	Demostrar la fiabilidad necesaria para prestar servicios de certificación.
	Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.
	Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.
	Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (continuación)	
OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN QUE EMITAN CERTIFICADOS RECONOCIDOS	Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios. de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.
	Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante quince años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.
	Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
	Seguro de responsabilidad civil por importe de al menos 3.000.000 de euros que podrá ser sustituido por: ◆ Aval bancario. ◆ Seguro de caución.

La Ley establece en su artículo 30, y disposición transitoria segunda, que los prestadores de servicios de certificación deberán comunicar al Ministerio de Industria, Turismo y Comercio, sus datos de identificación, los datos que permitan establecer comunicación con el prestador, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores de servicios de certificación (PSC) y la lista de los PSC que así lo han hecho se encuentra disponible en la dirección de Internet http://www.setsi.min.es.

Cuando un prestador de servicios de certificación vaya a cesar en su actividad debe comunicarlo con una antelación mínima de dos meses a los firmantes y a los solicitantes de los certificados de las personas jurídicas. Respecto de los certificados emitidos que estén vigentes a la fecha de su cese, los prestadores de servicios de certificación pueden bien transferir su gestión a otro prestador, siempre con el consentimiento expreso del titular del certificado y con la información previa de las características del prestador al que se tenga intención de transferir los certificados o bien extinguir su vigencia.

El régimen de responsabilidad de los prestadores de servicios de certificación se rige por las reglas generales de culpa contractual y extracontractual y recae sobre él la carga de la prueba de su actuación con diligencia.

El régimen sancionador que establece la Ley de firma electrónica diferencia entre sanciones muy graves, graves y leves y en concreto respecto de las infracciones que exponemos a continuación:

INFRACCIONES	SANCIONES
MUY GRAVES	
El incumplimiento de alguna de las obligaciones siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.	MULTA DE 150.001 € a 600.000 €
A excepción del incumplimiento de la obligación de constitución de la garantía económica.	
La expedición de certificados reconocidos sin realizar todas las comprobaciones previas cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.	
GRAVES	
El incumplimiento de alguna de las obligaciones, excepto de la obligación de constitución de la garantía cuando no constituya infracción muy grave.	MULTA DE 30.001 € a 150.000 €
La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica exigida por la Ley.	
La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en la Ley, en los casos en que no constituya infracción muy grave.	
El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de sus obligaciones si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.	
El incumplimiento por los prestadores de servicios de certificación de sus obligaciones respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la LOPD.	
La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Industria, Turismo y Comercio[47] en su función de inspección y control.	
El incumplimiento de las resoluciones dictadas por el Ministerio de Industria, Turismo y Comercio para asegurar que el prestador de servicios de certificación se ajuste a la Ley.	
LEVES	
El incumplimiento por los prestadores de servicios de certificación que no expidan certificados econocidos,de las obligaciones señaladas en el artículo 18 y las restantes de la Ley, cuando no constituya infracción grave o muy grave, excepto las contenidas en el apartado 2 del artículo 30.	MULTA DE HASTA 30.000 €

1.7. Camerfirma. Certificación digital de las Cámaras de Comercio (certificado electrónico gratuito)

1.7.1. AC Camerfirma SA.

Desde hace ya casi ocho años las Cámaras de Comercio trabajan en el ámbito de la certificación digital y la firma electrónica desde un proyecto empresarial llamado Camerfirma. Camerfirma fue creada conjuntamente con el Consejo Superior de Camaras en el 2000 con ayuda de varios socios del entorno bancario como Banesto, Caixa Galicia y Bancaja.

[47] *Tal y como venimos señalando, el Ministerio de Ciencia y Tecnología ha pasado a denominarse Ministerio de Industria, Turismo y Comercio. En este sentido, las referencias que se hagan a lo largo de este capítulo al Ministerio de Ciencia y Tecnología han de entenderse realizadas al Ministerio de Industria, Turismo y Comercio.*

Camerfirma emite certificados digitales de identidad empresarial, es decir establece siempre en sus certificados una vinculación contractual ente el titular y la entidad identificada en el certificado. La vinculación referida podría ser una vinculación de poder cuando el titular posee capacidad de representación de la entidad detallada en el certificado. En muchos casos es complejo trasladar al certificado esta capacidad de poder, principalmente debido a la gran variedad y complejidad de los poderes. Camerfirma por lo tanto decide incorporar la referencia del poder otorgado dentro de uno de los campos del certificado, de tal forma que la parte confiante sea capaz de validar si los poderes cubren los requerimientos de seguridad de una transacción electrónica concreta.

Camerfirma también ofrece otros tipos de certificados digitales: Los certificados de persona jurídica descritos por la Ley 59/2003, certificados de servidor seguro y de firma de código. Esta gama de productos cubre las necesidades de identificación electrónica empresarial necesaria para el desarrollo de servicios empresariales en redes abiertas como Internet.

El objetivo del proyecto Camerfirma por lo tanto es suministrar una identificación electrónica, ofreciendo información de la vinculación contractual entre personas físicas y jurídicas ya sea de poder o de simple pertenencia.

Para realizar estas tareas contamos con:

- *Un centro de datos propio especializado en la emisión de certificados. CPD en Ávila.*
- *Una red de Cámaras de Comercio que realizaran las labores de Autoridades de Registro.*

Las características especiales del producto son:

- **Certificados Empresariales.**
- **Certificados con perfil cualificado o reconocido** usados para la elaboración de firma electrónica avanzada. En aquellos certificados de persona física ya que el certificado cualificado o reconocido solo puede ser asociado a una persona física.
- **Certificados con amplio reconocimiento.** Para tener éxito en esta tarea tenemos que dotar a los certificados del mayor reconocimiento posible para lo cual Camerfirma ha trabajando conjuntamente con los distintos generadores de servicios electrónicos y aplicaciones.
  - Administración publica estatal.
  - Administración publica autonómica.
  - Administración Local (Ayuntamientos)
  - Navegadores (Microsoft).
- **Certificados de bajo coste** financiados por las Cámaras de Comercio

Otro de los aspectos importantes en la definición del producto es el proceso de creación y custodia de claves. En este aspecto Camerfirma elabora distintos circuitos distinguiendo el perfil del certificado, de la generación y el soporte de custodia de las claves criptográficas.

Los circuitos definidos para la elaboración de los certificados son los siguientes:

- Soporte software
  - Claves generadas por el usuario.
  - Claves generadas por el prestador del certificado.
- Soporte hardware
  - Claves generadas por el usuario.
  - Claves generadas por el prestador del certificado.

Esta información va asociada al identificativo de la política de tal forma que la aplicación conozca los aspectos sobre la generación y custodia de las claves y actuar en consecuencia.

ETIQUETA TIPO DE CERTIFICADO Y OID DE POLÍTICA	
CAM-PF-SW-KPSC	Certificado Cameral de persona física, claves almacenadas en software y generadas por el PSC 1.3.6.1.4.1.17326.10.6.2.1.1
CAM-PF-SW-KUSU	Certificado Cameral de persona física, claves almacenadas en software y generadas por el titular 1.3.6.1.4.1.17326.10.6.2.1.2
CAM-PF-HW-KPSC	Certificado Cameral de persona física, claves almacenadas en hardware y generadas por el PSC 1.3.6.1.4.1.17326.10.6.2.2.1
CAM-PF-HW-KUSU	Certificado Cameral de persona física, claves almacenadas en hardware y generadas por el titular 1.3.6.1.4.1.17326.10.6.2.2.2

Por otro lado dentro del contenido del certificado se incorporan los datos relativos a la autoridad de registro que ha realizado la validación de la información del usuario, y para los datos de representante o de persona jurídica el identificador de los poderes presentados.

Por último y para dar cumplimiento a la Ley 59/2003 se incluye un enlace a las declaraciones del titular para que este describa cualquier aspecto relevante en el uso del certificado.

Para la validación de los certificados Camerfirma pone a disposición de la parte confiante varios mecanismos entre los que se encuentran:

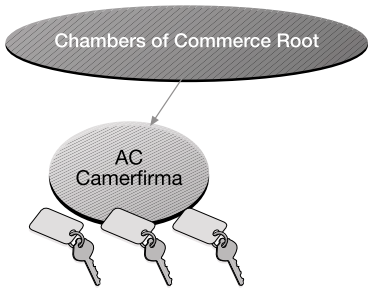
- CRL de acceso libre mediante acceso HTTP y LDAP.
- OCSP mediante el acceso a los servicios de Certiver.
- Webservice requerido por la Agencia tributaria.
- URL de revocación de Netscape.

Esta información se ofrece actualmente de forma libre y gratuita a aquellas personas que decidan confiar en los certificados emitidos por Camerfirma.

CARACTERISTICAS GENERALES DE LOS CERTIFICADOS:
Algoritmo de emisión: RSA 1024 bits
Versión x.509: V3
Uso de clave: Firma digital, Cifrado de clave, Cifrado de datos, Contrato de claves
Uso extendido de claves: Autenticación del cliente; Correo seguro
Tipo de certificado: cualificado / reconocido
Método de verificación de la identidad: presencial, realizada por personal adscrito a una organización Cameral.
Tipo de identificación para facturación: CIF IVA (VAT number as by article 28h of Directive 77/388/EEC), según artículo 28 nono de la Directiva 77/388/CEE, indicado en la extensión 1.3.6.1.4.1.17326.30.2.
Declaración del titular: el signatario puede realizar una declaración compatible con el artículo 11.3 de la Ley 59/2003 y con las políticas de certificación. El enlace a esta declaración estará contenido en la extensión bases del certificado del propio certificado (subject statment) y podrá contener declaración expresa de la indicación de autofacturación o facturación por cuenta de terceros.
Normas técnicas de referencia: RFC 3039 (IETF) y TS 101 862 (ETSI)

Para la emisión de los certificados antes referidos Camerfirma ha desarrollado una jerarquía de confianza llamada *Chambers of Commerce Root* cuya estructura se puede ver en la siguiente figura:

Jerarquía Camerfirma



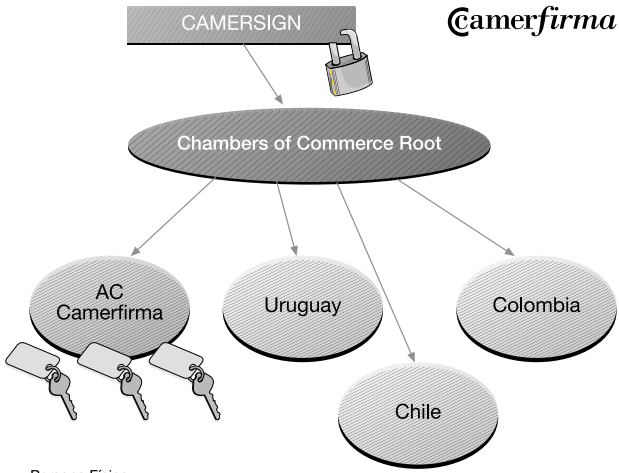
Esta jerarquía esta formada por una autoridad de certificación raíz fuente de la confianza para el resto de la estructura. Como autoridad delegada se encuentra AC Camerfirma que es la encargada de emitir certificados de identidad para la comunidad empresarial española.

Camerfirma tiene en este área un factor diferenciador fundamental que es su vocación internacional. El proyecto Camerfirma puede ser desarrollado internacionalmente en dos líneas principales:

- Primero: como parte de ampliación de la confianza al mercado latinoamericano.
- Segundo: mediante su incorporación a la Red de Confianza Cameral Europea “Chambersign”.

Nuestra visión es la comunicación electrónica segura de empresas de todo el mundo a través de una red de confianza Cameral. Esta visión encaja en el verdadero ámbito de Internet como medio de comunicación universal.

La figura anterior por lo tanto quedaría, incorporando estas nuevas áreas de desarrollo de la forma siguiente:



Camerfirma adicionalmente a la creación de certificados digitales desarrolla otra serie de áreas de negocio:

- Desarrollo e integración de aplicaciones con tecnología de Certificación digital.
- Outsourcing de PKI.
- Consultoría PKI.
- Desarrollo de productos de firma.
- Servicios de tercera parte de confianza:
  - Sellos de Tiempo.
  - Custodia de documentos.
  - Notarización de eventos electrónicos.

1.7.2. Proyecto "Hacia un Censo Digital"

La incorporación de la empresa española al uso de las Nuevas Tecnologías es una prioridad para las Cámaras de Comercio en la medida que es el principal pilar de crecimiento económico en la sociedad moderna y permite la creación de empleo sin efectos inflacionistas. En esta línea se está trabajando de una forma muy activa en actuaciones que impulsen y apoyen la incorporación y el uso de las Nuevas Tecnologías en las empresas, especialmente, en las pequeñas y medianas.

En este contexto, y dado el bajo nivel de penetración de la firma electrónica en estas empresas, la implantación de la misma constituye un elemento de gran importancia para apoyar y fomentar la incorporación de las Pymes a la Sociedad de la Información. Por este motivo se ha considerado prioritaria una actuación ambiciosa y global que ayude con eficacia a incorporar e incrementar el uso de la firma electrónica entre las empresas.

El objetivo que se propone es una acción de emisión masiva de identificadores digitales empresariales, con el objetivo de que las empresas españolas, y en especial la Pyme, puedan tener una identidad en la red. Dicha identidad estará basada en certificados digitales, y estará apoyada en el censo público de las empresas. Las Cámaras de Comercio según la Ley 3/1993[48], entre otras funciones de carácter público administrativo les corresponde llevar un censo público de todas las empresas así como de sus establecimientos, delegaciones y agencias radicados en su demarcación.

1.7.2.1. Objetivo del proyecto

El objeto del Proyecto es emitir gratuitamente 300.000 certificados digitales a empresas, desarrollando además usos de dichos certificados que estimulen el interés de las empresas y su uso creciente. Para ello, se desarrollará un programa coordinado de acciones dirigidas a un importante número de beneficiarios en los colectivos de Empresas, Pymes, micropymes y autónomos ***que impulse y apoye el uso de la certificación digital y la firma electrónica entre las empresas españolas.***

Este proyecto es una aportación fundamental de las Cámaras a la promoción de la sociedad del conocimiento, proporcionando a las empresas una herramienta básica que garantiza la seguridad en Internet. En esta misma línea se colabora con las Administraciones Públicas en la promoción de los servicios electrónicos, mediante la difusión de la certificación digital.

Actualmente 67 Cámaras participan en el proyecto, estas Cámaras actúan como autoridad de registro de Camerfirma que es la autoridad de certificación. Por esta función las Cámaras son las autoridades que validan los certificados digitales a las empresas de su demarcación.

[48] *Ley 3/1993, de 22 de marzo, básica de las Cámaras Oficiales de Comercio, Industria y Navegación.*

En esta publicación se adjunta un CD-WEB en el que se recoge toda la información para la solicitud de certificados digitales dentro del proyecto “Hacia un Censo Digital”, así como todo lo referente a sus usos y aplicaciones dentro de la vida empresarial.

El contenido de este CD-WEB es el siguiente:

CONTENIDO CD-WEB CAMERFIRMA

En el CD-WEB que se adjunta en esta publicación, se recoge toda la información necesaria para la obtención de una forma gratuita del certificado digital en sus distintas modalidades, así como toda la información y recursos para su uso.

En este CD hace referencia a los usos de los certificados Camerfirma, tanto desde el punto de vista de las Administraciones Públicas como de las propias Cámaras, además entre los usos empresariales hay que destacar la facturación electrónica. Para ello se recogen diferentes demostraciones de usos para poder observar de una manera práctica las utilidades del certificado.

LOS CERTIFICADOS DIGITALES: QUÉ SON, QUÉ PERMITEN HACER (Trámites con las Administraciones Públicas, Trámites con las Cámaras de Comercio, Usos Empresariales y Factura electrónica). MARCO LEGAL (Acceso a la ley de firma y Acceso a la directiva europea). CÓMO SE USAN (Office XP, Correo Electrónico, Ficheros Pdf, Dfirma Desktop y Servidores páginas HTML).

CERTIFICADO DE PERTENENCIA A EMPRESA (Cómo se firman los documentos, Descarga Dfirma Desktop, Solicita tu certificado y Cómo se gestiona un certificado digital). CERTIFICADO DE REPRESENTANTE / PERSONA JURÍDICA (Cómo se firman los documentos, Descarga Dfirma Desktop, Solicita tu certificado y Cómo se gestiona un certificado digital). CERTIFICADO DE FIRMA DE CÓDIGO / SERVIDOR SEGURO.

En línea con estos recursos, el CD se completa con exposición del marco legal y de las especificaciones de cada uno de los certificados digitales para empresas. Así mismo recoge enlaces de interés, y videos demostrativos tanto de firma de documentos como de pasarelas de autenticación.

2. PAGO ELECTRÓNICO

2.1. Consideraciones generales

Los llamados medios de pago electrónico son aquellos sistemas que permiten el procesamiento de órdenes de pago a través de sistemas electrónicos.

El pago electrónico no debe confundirse con la transferencia electrónica de fondos, como elemento que precede al pago electrónico pero que no siempre se concreta en él, pues puede ser una simple transacción sin objeto de pago.

En definitiva, no puede existir pago electrónico sin transferencia electrónica de fondos pero no toda transferencia electrónica de fondos es un pago electrónico.

Así, la transferencia electrónica implica una actividad económica por medios electrónicos que puede ser, además de un pago, una retirada de dinero o un depósito.

Dentro de los medios de pago electrónico encontramos distintos supuestos como son el pago mediante tarjeta, el pago por medio de cheque electrónico, el pago a través de transferencia electrónica, en el caso en el que como hemos analizado ésta tenga por fin realizar un pago, o el pago mediante dinero electrónico.

Atenderemos al pago mediante tarjeta por ser uno de los medios de pago electrónico más utilizado, pasando antes a explicar brevemente otros medios que hemos señalado.

En primer lugar y respecto de los cheques electrónicos, diremos que son instrumentos de pago que evitan el desembolso de numerario en las transacciones mercantiles. Por medio del cheque, el que lo emite, dispone de los fondos de su cuenta bancaria a favor de un tercero acreedor.

El hecho de que el cheque sea electrónico deriva de los medios a través de los que se elabore. Con este carácter, será un instrumento de pago basado en el acceso directo a una cuenta bancaria de la que es titular el usuario de aquél con el fin de realizar pagos por Internet.

En la normativa y costumbre española su uso no está extendido, en primer lugar porque su regulación exige unas formalidades concretas y también porque no existe una cultura de uso de estos medios, al contrario que en otras sociedades como la francesa o la estadounidense.

En segundo lugar, las transferencias electrónicas ya hemos comentado que pueden suponer un pago o no, y en el caso de que lo sean supone una liberación de una deuda, dado que cumple la función de pago mediante el traspaso del dinero de su cuenta de origen a la de destino.

En lo que respecta al dinero electrónico como medio de pago, no debe ocupar nuestra atención ya que en la actualidad el dinero electrónico se encuentra en fase de desarrollo existiendo varios sistemas y se encuentra recogido en distintas reglamentaciones, comunitarias y nacionales [49] pero aun es pronto para describir los cambios que traerá la utilización de un instrumento electrónico de pago que cumpla con todas las características del dinero tradicional –entre otras, anonimato y carácter fungible–, pero de forma electrónica.

Visto esto, entremos a analizar el pago electrónico realizado mediante tarjeta en el que, teniendo en cuenta el funcionamiento de la firma electrónica, vamos a estudiar el caso de que a ésta se le una la utilización de pago por medios electrónicos, con el aprovechamiento de la seguridad ofrecida por las técnicas criptográficas, que permiten que los datos de pago "viajen" seguros a través de la red y garantizan la integridad, conservación y autenticación de los documentos transmitidos, así como la identificación inequívoca de los intervinientes en la contratación, abriéndose un camino sencillo, ágil, seguro y, hoy en día, idóneo para la utilización de estas técnicas en el comercio electrónico a través de Internet.

2.2. Pago mediante tarjeta

Uno de los medios de pago electrónico más arraigados en la sociedad es el pago por tarjeta. El conocido dinero de "plástico" se presenta en una tarjeta que incorpora una banda magnética o un microchip que permite a su titular realizar una serie de operaciones, tanto con la entidad emisora, como con terceros, con objeto de llevar a cabo un pago.

El pago mediante tarjeta *no implica necesariamente que la compra del bien o el pago del servicio se esté realizando a través de Internet,* pero en el caso de que esto sea así se asimila a una venta a distancia por lo que le sería de aplicación, en lo que no esté previsto en la LCE, la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista [50] (en adelante LOCM).

La citada LOCM dispone en su artículo 46 que

> *Cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad.*

[49] *En nuestro país la ley financiera ha sido aprobada mediante la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, publicada en el Boletín Oficial del Estado núm. 281, de 23 de noviembre.*

[50] *Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, publicada en el Boletín Oficial del Estado núm. 15, de 15 de enero, que ha sido modificada por la Ley 47/2002, de 19 de diciembre, publicada en el Boletín Oficial del Estado núm. 304, de 20 de diciembre.*

Esta consideración no está exenta de precauciones dirigidas a evitar el fraude por el titular de la tarjeta porque en su segundo apartado dispone que si el titular hubiese hecho el pago y pidiese después su anulación responderá ante el vendedor por los daños y perjuicios que hubiese podido causar.

2.3. Protocolos de seguridad

En el caso de las transacciones electrónicas, y como ya hemos señalado, son la desconfianza y el miedo a la falta de seguridad en el envío y recepción de la orden de pago, las principales causas que paralizan, o por lo menos no impulsan, el comercio por Internet.

Uno de los medios que tratan de evitar esta traba al comercio electrónico son los protocolos de seguridad.

Éstos son soluciones tecnológicas que buscan asegurar que los datos relativos a una transacción comercial puedan ser transmitidos al comerciante de forma segura.

Los dos protocolos de seguridad más generalizados son el SSL y el SET.

En primer lugar, el protocolo SET o *Secure Electronic Transactions,* ofrece autenticación a todas las partes implicadas, confidencialidad e integridad. Esto es así porque este protocolo de seguridad se basa en una infraestructura de clave pública que le dota de estas características.

Pese a la gran seguridad que presenta este medio tecnológico, no son pocas las dificultades que presenta en su utilización pues entre otras cosas implica la instalación de un software específico *(wallet).*

Por su parte, el protocolo de seguridad *Secure Sockets Layer, conocido como SSL,* consiste en la creación de un canal seguro de comunicación a través de Internet entre el comerciante y el comprador.

El efecto que produce es el de la autenticación del servidor, la encriptación de los datos y la integridad del mensaje que se remite a través del canal.

Las consecuencias de estos efectos son las de suponer una garantía para el comprador al autenticar al comerciante y la de que los datos se transmitan cifrados.

capítulo tercero

Propiedad intelectual y nombres de dominio

1. PROPIEDAD INTELECTUAL E INDUSTRIAL

Uno de los activos patrimoniales más importantes que tiene cualquier empresa, con independencia de cuál sea su dimensión, es el de los bienes inmateriales constituidos por las creaciones intelectuales (propiedad intelectual) y sobre signos distintivos que permiten distinguir sus bienes y servicios en el mercado (propiedad industrial) además, en su caso, de las creaciones industriales que puedan desarrollar. Es así como, de un lado, la propiedad intelectual y, de otro lado, la propiedad industrial, se convierten en aspectos fundamentales que necesitan de protección en el ámbito empresarial.

1.1. Introducción

Íntimamente unido a lo anterior se encuentra en el entorno electrónico, y en particular en Internet, el uso de los nombres de dominio, identificadores electrónicos de las empresas que permiten a éstas identificarse en Internet de manera que los usuarios y, en su caso, clientes, pueda acceder a sus sitios o páginas web a través de la marca u otro signo, con el que vienen siendo ya conocidos en el entorno físico.

Por último, la actividad diaria de cualquier empresa requiere del uso de bienes y/o servicios informáticos, lo que determina la necesidad de negociar y elaborar contratos que regulen las obligaciones de las partes, por un lado, el usuario y, por otro lado, el prestador del servicio o suministrador del bien de que se trate.

A continuación, vamos a atender a cada una de estas cuestiones con la intención de incidir en los aspectos más relevantes que una empresa tiene que tener presente en cada uno de estos ámbitos.

1.2. Propiedad intelectual

La propiedad intelectual, regulada por el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprobó el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, en adelante LPI, tiene por objeto la protección de *una obra literaria, artística o científica*, y la persona que gozará de la protección será su autor, que, como norma general, será siempre una persona natural, aunque en los casos previstos por la Ley se podrá beneficiar también una persona jurídica.

Los derechos de protección que atribuye la legislación de propiedad intelectual se clasifican en dos tipos: derechos morales y derechos patrimoniales. Mientras los derechos personales son irrenunciables e inalienables, los derechos patrimoniales son susceptibles de transmisibilidad.

Las obras pueden ser de varios tipos, y así se entienden los distintos casos de protección que la Ley otorga a personas jurídicas.

Las obras pueden ser independientes, en colaboración, colectivas o compuestas.

Se presumirá autor, salvo prueba en contrario, a quien aparezca como tal en la obra. Es decir, que por el simple hecho de "firmar" una obra, y mientras no se demuestre lo contrario, esa persona será considerada autor y gozará de la protección de la Ley.

No será necesario que el autor señale su nombre completo, sino que bastará con cualquier signo que lo identifique, incluyendo el de su propia firma.

Cuando una obra se divulgue en forma anónima o bajo pseudónimo o signo, el ejercicio de los derechos de propiedad intelectual corresponderá a la persona natural o jurídica que la saque a la luz, mientras el autor no revele su identidad, y siempre y cuando la persona que lo haya sacado a la luz tenga el consentimiento del autor.

1.3. Propiedad industrial

Los derechos de propiedad industrial permiten la protección de determinados signos distintivos de la actividad empresarial, con el objeto de que las personas que acudan a unos servicios conozcan, sencillamente por dichas marcas o signos distintivos, el empresario que se encuentra tras ellos, y quien, al final, responderá de ellos.

Además, existen determinadas creaciones que encuentran su acomodo natural dentro de los derechos de propiedad industrial. El Estatuto de la Propiedad Industrial [51] la define como *la que adquiere por sí mismo el inventor o descubridor con la creación o descubrimiento de cualquier invento relacionado con la industria, y el productor, fabricante o comerciante con la creación de signos especiales con los que aspira a distinguir de los similares los resultados de sus trabajos* (art.1).

Vemos que la diferencia fundamental con las creaciones intelectuales, siendo ambas creaciones o descubrimientos, en principio radica en la relación del invento con la industria.

Es éste, por lo tanto, el hecho primero diferenciador, para comprender si un bien es objeto de protección intelectual o industrial.

Sin embargo, las diferencias son mucho mayores según vamos profundizando en la materia, puesto que lo que realmente otorgan los derechos de propiedad industrial es un derecho de uso o explotación exclusiva.

Las creaciones intelectuales, como hemos señalado anteriormente, otorgan dos tipos de derechos, personales y patrimoniales, y precisamente estos últimos serán los que tengan una mayor facilidad de cesión.

Los derechos de propiedad intelectual no se entiende que tengan como fin último su explotación, sino, bien al contrario, el reconocimiento del autor de una obra como tal, pasando la explotación de la misma a un segundo plano, en la filosofía de la Ley.

Sin embargo, los derechos de propiedad industrial tienen, como fin último, el reconocimiento de la explotación de un invento por parte de su creador, con los consiguientes beneficios patrimoniales que ello supone.

[51] *Estatuto sobre Propiedad Industrial, aprobado por Real Decreto-ley de 26 de julio de 1929 (Gaceta núm. 127, de 7 mayo 1930).*

Podríamos decir que la diferencia entre los bienes protegibles mediante los derechos de propiedad intelectual y los derechos de propiedad industrial es que, mientras la primera se centra en las creaciones artísticas, la segunda se centra en las cosas susceptibles de ser utilizadas.

Mientras que para la propiedad intelectual no es requisito necesario que el bien objeto de protección tenga alguna utilidad, sí lo será para los bienes objeto de propiedad industrial.

Los derechos de propiedad industrial poseen, además, una segunda parte, más diferenciada de los derechos de propiedad intelectual, pero que debemos considerar de igual o similar importancia, como es la de evitar la confusión de los resultados de un trabajo por parte de los potenciales clientes o consumidores.

Tan importante como el hecho de poder explotar un invento relacionado con la industria por parte de su autor debemos considerar el de que no se confunda un negocio o una creación con la de otro empresario distinto.

El art. 2 del Estatuto de la Propiedad Industrial indica que el derecho de propiedad industrial puede adquirirse por virtud del registro de las patentes, de las marcas, de los nombres comerciales, de los modelos y de los rótulos de establecimiento.

Todas las formas de protección citadas responden a los distintos elementos que la legislación sobre propiedad industrial pretende proteger para el buen funcionamiento de la industria.

1.4. Protección jurídica de los programas de ordenador

En las empresas es muy común que los programas de ordenador constituyan una parte muy importante de su activo, e, incluso, que hayan desarrollado ellas mismas sus propios programas que les permitan optimizar su actividad, para conseguir los máximos beneficios.

Estas empresas llevan a cabo su actividad con la transmisión de información como su principal labor pero, a la vez que para la transmisión de la información es necesaria la utilización de programas de ordenador, no se puede obviar la necesidad de protección jurídica que esos programas necesitan.

Además, respecto a los programas de ordenador nos encontramos con otro problema añadido, y es el de la incardinación de los mismos dentro de un ámbito de protección o de otro; esto es, a la protección de los programas de ordenador mediante las normas de propiedad intelectual, como creaciones del intelecto que son, o mediante las normas de propiedad industrial como parte integrante de una máquina.

En la Unión Europea los programas de ordenador se protegen como bienes de propiedad intelectual, mediante los derechos de autor. Y es que el que el software es producto de una actividad creativa, con una gran carga de intelectualidad es algo que, en principio nadie discute.

Lo que también es un hecho es la necesidad de implantar ese software en una máquina que permita su funcionamiento y que esa máquina encuentra su protección dentro de los derechos de propiedad industrial (patentes), es algo que tampoco se puede poner en duda.

En nuestra legislación, estos programas encuentran protección en el título VII del Real Decreto Legislativo 1/1996, de 12 de abril por el que se aprobó el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia que se rubrica, además, “De los programas de ordenador”.

Sin embargo, si el programa de ordenador forma parte de un procedimiento completo, susceptible de ser patentado, dicho programa se encontrará dentro de la protección de la patente, lo que de nuevo indica las dudas que al respecto de la protección tienen nuestros legisladores.

Además, la tendencia dentro de la Unión Europea no está tan definida como pudiera parecer, a favor de la protección de los programas de ordenador mediante los derechos de propiedad industrial. En este sentido, todavía se está debatiendo en la Unión Europea, tras un amplio período de consulta, la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la patentabilidad de las invenciones implementadas en ordenador [COM(2002) 92 final] en la que se analiza la situación actual en materia de patentabilidad de dichas invenciones implementadas en ordenador en el ámbito de la Unión Europea y en particular conforme a la práctica seguida por la Oficina Europea de Patentes.

La Propuesta de Directiva lleva también a cabo una comparación con otros sistemas, en particular, Estados Unidos y Japón, en los que los programas de ordenador sí son patentables, lo que determina que haya posturas, en particular la de las grandes compañías de la industria del software, que defienden la patentabilidad del software frente a la posición de los fabricantes y usuarios de software libre y de fuente abierta *(open code)* que se oponen firmemente a esta Propuesta por entender que ello podría restringir el acceso a la creación de programas de ordenador.

En concordancia con la primera Directiva 91/250/CEE del Consejo, de 14 de mayo, sobre la protección jurídica de programas de ordenador, podemos encontrar en la legislación interna una serie de principios que rigen esta protección; así y siguiendo los criterios indicados por la Comisión Europea en su informe sobre la transposición de la Directiva 91/250/CEE indicada (COM (2000) 199 final):

- *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 la LPI a la enumeración de una serie 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.*

a. Concepto de programa de ordenador

Como ya hemos indicado y a efectos de su inclusión en el ámbito de protección conferido, la LPI define el 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".*

Además, incluye en el ámbito de protección conferido a los programas de ordenador la documentación preparatoria que acompaña al programa de ordenador, entendiendo por tal los manuales técnicos y de uso de los programas de ordenador; y a las versiones sucesivas así como a los programas derivados.

Respecto de los requisitos exigidos por la LPI a efectos de otorgar la protección conferida en materia de derechos de propiedad intelectual, se concretan en la necesidad de 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 manifieste dicha creación intelectual.

La protección conferida a los programas de ordenador no abarca sólo a éstos sino que se extiende también a las versiones sucesivas de un programa de ordenador original y los programas derivados del mismo, con la única excepción de que el programa de ordenador haya sido creado para ocasionar algún efecto nocivo en un sistema informático, es decir, que se trate de un virus.

Expresamente excluye la LPI del ámbito de protección conferido a los programas de ordenador las ideas y principios que sirven de base para la creación de los elementos de un programa de ordenador, así como los que sirven de fundamento a sus interfaces. También se excluye de esta protección a los programas de ordenador creados para causar daños, es decir, los virus informáticos.

Sin reiterar aquí de nuevo lo ya expuesto respecto de la protección conferida por la LPI, cabe señalar que existen otras normas del ordenamiento jurídico que también ofrecen protección a los programas de ordenador, así cabe señalar principalmente el Código Penal de 1995, en materia de delitos contra la propiedad intelectual (arts. 270 a 272), y la Ley 11/1986, 20 de marzo, de régimen jurídico de Patentes de Invención y Modelos de Utilidad, si bien no es objeto de este apartado analizar la patentabilidad del software.

Respecto de la protección conferida por el Código Penal, los programas de ordenador quedarían protegidos en el mismo régimen previsto para los delitos cometidos contra la propiedad intelectual, tipificando expresamente en su artículo 270 las conductas consistentes en:

- La fabricación
- Puesta en circulación
- Tenencia

De cualquier medio que se destine específicamente a facilitar:

- La supresión no autorizada
- La neutralización

De cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Sin perjuicio de la protección penal conferida y que resulta, al igual que las demás vías previstas, complementaria a lo que dispone la LPI en materia de propiedad intelectual, y que debe encuadrarse dentro de las propiedades especiales reconocidas por el Código Civil, cabe señalar que esta última dispone expresamente otra forma más de protección para aquellos programas de ordenador que formen parte de una patente o modelo de utilidad, que no es sino la protección conferida en virtud de la aplicación de la normativa vigente en materia de protección industrial.

b. Otras vías de protección

Debemos referirnos en este apartado principalmente a la protección de carácter administrativo, y más en concreto registral, en virtud de la posibilidad de que los programas de ordenador accedan al Registro de la Propiedad Intelectual, que tiene por objeto la inscripción tanto de éstos como de sus sucesivas versiones y los programas derivados.

Si bien es posible la inscripción de programas de ordenador en dicho Registro, cabe señalar que en ningún momento ésta tiene carácter constitutivo, sino que proporciona:

- **Publicidad** frente a terceros de los derechos inscritos en el mismo.
- 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.

De esta manera se crea una presunción sobre la existencia de los derechos inscritos en el mismo, si bien cabe prueba en contrario, por lo que se convierte en una protección más bien de carácter formal.

c. Registro General de Propiedad Intelectual

Cualquier obra susceptible de ser protegida mediante los derechos de autor, puede ser inscrita en el Registro General de la Propiedad Intelectual.

La inscripción de las obras en este Registro es potestativa, es decir, que al contrario que para la protección mediante los derechos de propiedad industrial, no es necesaria la inscripción en el Registro para que la protección de la obra surta efecto.

Este Registro, como todo lo relativo a la propiedad intelectual, depende del Ministerio de Cultura.

Los requisitos que se exigen para la presentación de programas de ordenador, en la actualidad, son:

REQUISITOS GENERALES

A. **Impreso oficial** de solicitud por **duplicado,** acompañado de:
   - **Fotocopia del Documento Nacional de Identidad:**
     a.1.- Del autor.
     a.2.- Del titular de los derechos patrimoniales inscribibles.
   - Si se trata de **personas jurídicas,** habrá de aportarse:
     b.1.- El título que acredite su personalidad jurídica.
     b.2.- El Código de Identificación Fiscal (CIF).
   - Si se actúa mediante **representante,** éste deberá aportar el documento que acredite dicha representación de forma fehaciente.

B. **Ejemplar identificativo del programa de ordenador.** (ver siguiente cuadro explicativo).

C. **Justificante de Pago** de la Tasa correspondiente.

D. **Documentación complementaria** requerida en virtud de la legislación sobre propiedad intelectual, si la hubiera. (ver siguiente cuadro explicativo).

EJEMPLAR IDENTIFICATIVO DEL PROGRAMA DE ORDENADOR (PUNTO B CUADRO ANTERIOR)

A. Programas de ordenador **inéditos:**
   - La **totalidad del código fuente,** en CD-ROM o en soporte papel, debidamente encuadernada y paginada. (En la Oficina Provincial de Madrid, se permite su presentación en disquete/s de 3 $^{1}/_{2}$ pulgadas, en código ASCII sin que necesite tratamiento previo -sin comprimir, proteger de lectura, etc.-). En la etiqueta figurará el nombre del programa y el autor.
   - Un ejecutable del programa.
   - Opcionalmente, podrá presentarse una memoria que contenga:
     – Una breve descripción del programa de ordenador.
     – El lenguaje de programación.
     – El entorno operativo.
     – Un listado de ficheros.
     – El diagrama de flujo.
     – En su caso, número de depósito legal.
   - Cuando la extensión del código fuente o las condiciones de archivo lo hicieran necesario, el registro podrá exigir que dicho código se aporte en CD-ROM u otro soporte diferente.

B. Programas de ordenador **editados**
   - Resumen de al menos 20 folios del código fuente, que reproduzcan elementos esenciales del mismo, encuadernado y con el nombre del programa y el autor.

DOCUMENTACIÓN COMPLEMENTARIA EN LOS SUPUESTOS DE TRANSMISIÓN DE DERECHOS (PUNTO D DEL PRIMER CUADRO)

A. Si se desea **inscribir los derechos** sobre una obra a favor de persona **distinta del autor,** se debe aportar:

Contrato de cesión de derechos, salvo que el programa lo hubiera realizado un asalariado por cuenta ajena.

- Sólo se inscribirá en virtud de documento público ante notario.
- Escritura expresará los derechos cedidos, las modalidades de explotación, el tiempo, el ámbito territorial y el carácter exclusivo o no.
- Justificante de pago del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados, o el justificante de exención expedido por la Hacienda Pública.

B. Respecto a los programas creados por **trabajadores asalariados por cuenta ajena, y en virtud de esa relación laboral** se precisa:

Declaración donde conste que el programa se ha creado en virtud de esa relación laboral, **en documento público,** salvo que la haga el propio trabajador, en la que bastará una **legitimación notarial de la firma,** o que ésta **se extienda ante el funcionario del Registro.**

1.5. Protección jurídica de las bases de datos

En lo que hace referencia al comercio electrónico, es necesaria la utilización de la información para el desarrollo de la actividad, de una manera, además, lo más eficiente posible.

Si conseguimos tratar la información –elemento básico de una actividad que se desarrolle a través de la Red, y en la que no existe un trato presencial o físico con los clientes–, de una manera más eficiente que la competencia, tendremos una ventaja incalculable sobre ésta.

Por otra parte, si desarrollamos una base de datos que produzca un tratamiento eficaz de esa información, es muy posible que existan otras empresas en el mercado que deseen implementarla a su actividad, por lo que se nos antoja imprescindible el desarrollo de una protección adecuada para este tipo de herramientas.

Las bases de datos son, dicho 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.

Los documentos no tienen por qué ser propiedad de la misma persona que crea la propia base de datos. Son objetos distintos, y la protección que se confiere a ambos elementos también será distinta.

Las bases de datos, en función del tipo de acceso las podemos clasificar en bases de datos **autónomas** (o de acceso local, desde el lugar en que nos encontremos utilizando el ordenador, normalmente la base de datos se encontrará en un CD-ROM o un DVD-ROM) o bases de datos *on line*, (a las que accederemos de manera remota, y que se encontrarán en un servidor común).

a. Forma de protección

Las bases de datos son obras de creatividad intelectual: nos estamos refiriendo a las propias bases de datos, es decir, a la estructura que contiene la información.

Las bases de datos se protegen como obras de creatividad intelectual, ya que esta creatividad no se puede poner en duda en dos momentos distintos, tanto en el almacenamiento de información como en la recuperación de la información.

Este esfuerzo que se debe hacer para poder poner en el mercado una herramienta de tratamiento de la información agrupada se ve, de esta manera, protegido contra los posibles ataques que pueda sufrir.

La copia o el acceso a las bases de datos se puede hacer a un coste sensiblemente inferior al de su creación y desarrollo, por lo que es preciso que la protección de estos productos sea lo más adecuada posible al bien objeto de protección.

De forma análoga a como ocurría con los programas de ordenador, el objeto de protección no es solamente la recopilación de información, sino más bien todo el procedimiento de creación de una base de datos y el resultado del mismo.

En este mismo sentido, otro motivo por el que la protección debe ser a la propia base de datos y no al contenido de la misma, es el de que es un producto que puede sufrir múltiples actualizaciones, que, además, impliquen un cambio sustancial en el contenido, lo que conllevaría una indefinición de la protección. Por este motivo, la protección debe ser a la propia base de datos (a su estructura), y no a su contenido.

La protección de la estructura de la base de datos se entiende como *forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos*.

Si bien al igual que en los programas de ordenador, son principalmente las inversiones efectuadas por el sector privado las que requieren de la protección conferida por la Ley, la verdadera diferencia, señalada en la Exposición de Motivos de la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (publidada en el B.O.E. núm. 57, de 7 de marzo de 1998), la constituye el hecho de que las diferencias en su protección jurídica en los diferentes Estados miembros de la Unión Europea *incide de forma directa y negativa en la libertad de las personas físicas y jurídicas de suministrar bienes y prestar servicios en el sector de las bases de datos.*

De esta forma el legislador nacional procedió a dar cumplimiento al mandato comunitario, si bien la Ley se incorporó directamente a la normativa existente, recuérdese que es la LPI, sobre propiedad intelectual bajo razones de eficacia y economía legislativa.

Además de lo anterior, cabe señalar que las bases de datos cobran especial importancia debido a la inversión cuantitativa y cualitativa que se produce en las mismas, por parte de su fabricante, materializada en una inversión sustancial de factores tales como:

- Medios financieros
- Empleo de tiempo
- Esfuerzo
- Energía
- Otros de similar naturaleza

si bien los mismos serán sometidos a examen previo, a efectos de conferir la correspondiente protección por parte del ordenamiento jurídico.

Respecto del concepto de base de datos, cabe señalar que la Ley considera base de datos:

> *"Las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma".*

De esta forma se confiere protección a las bases de datos tanto *on line* como *off line*.

- Doble ámbito de protección

Como ya hemos señalado la protección jurídica de las bases de datos goza en nuestro ordenamiento jurídico de una previsión específica en la Ley 5/1998, de 6 de marzo, que contempla una doble vía de protección, en cualquier caso legal, al afirmar la aplicabilidad sobre la base de datos tanto de la citada Ley como de la LPI.

Se articula por tanto un doble ámbito de protección, de un lado, el que confiere el derecho de autor, y de otro lado, el derecho *sui generis,* como figura jurídica creada de forma específica por la Ley 5/1998 al transponer a nuestro ordenamiento jurídico la Directiva 96/9/CE. Sin perjuicio de la exposición que se realizará sobre el derecho *sui generis,* cabe señalar que el derecho de autor recae sobre la base de datos. De manera que ambos derechos o medidas de protección resultan ser complementarias.

Este derecho de autor requiere del requisito de originalidad, al igual que con el resto de obras que gozan de la protección conferida por los derechos de propiedad intelectual, en la selección o disposición de sus contenidos, y sin perjuicio, ya que los mismos quedan excluidos de la protección conferida por esta norma remitiéndose, en su caso, a la norma específica que dote de protección a las mismas, así:

- Las relativas a otros derechos de propiedad intelectual
- El derecho *sui generis*
- Derecho de propiedad industrial
- Derecho de la competencia
- Derecho contractual
- Normativa sobre secretos
- Protección de datos de carácter personal
- Protección de los tesoros nacionales
- Normativa sobre el acceso a documentos públicos

Son por tanto materias que, por conformar el contenido de la base de datos, no reciben la protección conferida a la misma y que reciben en su caso una protección específica en función de la materia de que se trate.

De igual forma, la protección conferida por el derecho de autor tampoco se extiende a los elementos que resulten necesarios para:

- el funcionamiento o
- la consulta de algunas bases de datos como el tesauro y los sistemas de indexación.

Respecto de estos últimos cabe señalar que sí serían objeto de protección por parte del derecho *sui generis*.

- Derecho sui generis

El derecho *sui generis* constituye una figura específica, surgida en nuestro ordenamiento jurídico por efecto de la transposición de la normativa comunitaria en la materia, y que en ningún caso se contrapone o resulta incompatible con la protección legal conferida en virtud de la normativa sobre propiedad intelectual.

Esta figura jurídica tiene por objeto la protección en una base de datos de:

- La inversión sustancial
- Evaluada cualitativa o cuantitativamente
- Realizada por su fabricante
- De cualesquiera medios tales como tiempo, esfuerzo, energía u otros similares
- Para la obtención, verificación o presentación de su contenido

Asimismo, la protección conferida por el derecho *sui generis* también recaería sobre las modificaciones sustanciales posteriores que se produjeran en una base de datos, siempre que las mismas cumplan todos los requisitos para otorgar dicha protección a una base de datos.

En consecuencia, el titular del derecho *sui generis,* y por tanto beneficiario de la protección conferida por el mismo, es el fabricante de la base de datos. Si bien para gozar de la protección conferida por aquél es necesario que concurran una serie de requisitos a fin de que el mismo pueda ser válidamente reivindicado, y que ya se han señalado.

Cabe señalar, que al igual que ocurre con el derecho de autor, la protección conferida en virtud del derecho *sui generis* es independiente de la protección conferida a su contenido por la legislación que resulte aplicable.

Respecto de las características del derecho *sui generis* debe destacarse que el mismo no se configura como un derecho absoluto, sino que al igual que ocurre con otros derechos éste no es absoluto, sino que se prevén expresamente una serie de excepciones legalmente tasadas al mismo por parte del usuario legítimo.

Este derecho no surge sino en el mismo momento en que finaliza el proceso de creación o fabricación de la base de datos, y no con carácter previo al mismo, teniendo una duración de 15 años desde el día 1 de enero del año siguiente en que terminó dicho proceso.

En definitiva, el objeto de protección del derecho *sui generis* son las importantes inversiones de naturaleza económica que han sido efectuadas previamente por el fabricante de la base de datos, y que de no ser así serían fácilmente vulnerables por la posibilidad de efectuar copias con un bajo coste.

2. NOMBRES DE DOMINIO

2.1. ¿Qué es un nombre de dominio?

En un principio los ordenadores conectados a Internet se comunicaban entre sí a través de las direcciones IP *(Internet Protocol),* direcciones que identifican a los ordenadores compuestas por cuatro bloques de números separados por puntos que van desde el 0 hasta el 255, (por ejemplo 232.125.96.205). Conforme la red iba creciendo, recordar un conjunto de números se fue haciendo cada vez más complicado y de este modo se creó el sistema de los nombres de dominio, nombres fáciles de recordar que los identificaban con la dirección IP de manera que ya no era necesario recordar el número de la misma.

Actualmente los nombres de dominio cumplen una función de identificación comercial entrando así a actuar en el ámbito comercial y coincidiendo de esta forma con otros identificadores comerciales como son las marcas. Entendemos por marca todo signo o medio que diferencia o sirva para diferenciar en el mercado productos o servicios de una persona de productos o servicios similares de otra persona. En concreto, pueden constituir marcas las palabras o combinaciones de palabras, incluidas las que sirvan para identificar a las personas. Éste es uno de los principales motivos por el que se suscitan con-

troversias puesto que los nombres de dominio facilitan el acceso a las páginas web y, en muchas ocasiones, permiten asociar dicho nombre de dominio a la entidad que lo ha registrado para que su imagen e identidad sea conocida en el entorno electrónico como lo es fuera de él.

La composición de una dirección de Internet nos muestra la clasificación de los nombres de dominio y ésta la podemos analizar a través del siguiente ejemplo:

http//: www.cscamaras.es

- **http://**, es el protocolo de comunicaciones que se utiliza en Internet *(HyperText Transfer Protocol)* y que permite al usuario ver páginas web en la pantalla de su navegador;
- **www**, servicio de Internet *(World Wide Web);*
- "**cscamaras**", es el nombre que se registra bajo el dominio correspondiente, es elegido por el usuario y se asocia al mismo, y permite acceder al sitio web de la entidad que lo ha registrado;
- "**.es**", es el dominio bajo el que se registra un nombre. En este caso se trata de un nombre de dominio de primer nivel de código de país correspondiente a España.

La clasificación de los nombres de dominio se realiza atendiendo a la proximidad que tienen con el final de la dirección de Internet, así serán nombres de dominio de primer nivel los que se encuentren al principio de la dirección mirando ésta desde la derecha. En el caso que hemos puesto de ejemplo, el nombre de dominio de primer nivel es el ".es", como nombre de dominio de segundo nivel encontramos "cscamaras", nivel éste en el que surgen las controversias con otros identificadores comerciales, a las que anteriormente nos hemos referido.

Los nombres de dominio de primer nivel son conocidos como los *Top Level Domain* (TLD) y los de segundo nivel como los *Second Level Domain* (SLD).

Los nombres de dominio de primer nivel se dividen en dos grupos: nombres de dominio de primer nivel genérico (gTLD, *generic Top Level Domain)* y nombres de dominio de primer nivel de código país (ccTLD, *country-code Top Level Domain).* Por último, están los nombres de dominio de tercer nivel, tales como ".com.es", ".gob.es" o ".nom.es".

Los nombres de dominio de primer nivel genéricos son los que recogemos a continuación. Hasta el momento se han creado catorce nombres de dominio genéricos y han ido surgiendo atendiendo a las necesidades del tráfico jurídico:

gTLD	Acceso	Finalidad
.com	Libre	Comercial
.net	Libre	Comercial
.org	Libre	Organizaciones
.mil	Restringido. Organismos militares del ejército de los Estados Unidos	Militar
.int	Organizaciones internacionales sin límite	Organizaciones internacionales
.edu	Restringido. Organizaciones educativas superiores	Educación
.gov	Restringido. Organismos de gobierno	Gobierno

gTLD	Acceso	Finalidad
.biz	Empresarios	Exclusivamente comercial y empresarial
.info	Libre	
.pro	Restringido. Profesionales de determinadas categorías	Profesionales pertenecientes a un colegio profesional o similar organización administrativa
.name	Libre. Personas físicas	Identificación de personas físicas
.aero	Restringido. Industria aeronáutica	Industria aeronáutica
.coop	Restringido. Cooperativas	Identificación cooperativas
.museum	Restringido. Museos	Museos

Por su parte, los nombres de dominio de código país se componen de dos caracteres que derivan de las Normas ISO 3166 y, por lo que respecta a España el ccTLD es ".es". La entidad encargada del registro de este nombre de dominio es la Entidad Pública Empresarial Red.es, que depende del Ministerio de Industria, Turismo y Comercio [52].

Los nombres de dominio de segundo nivel (SLD, *Second Level Domain*) son los que habitualmente pueden coincidir con la marca o con el nombre comercial y los que dan lugar a la mayoría de los conflictos en materia de nombres de dominio.

El nombre de dominio de código país correspondiente a España, el ".es", es regulado por el Plan Nacional de nombres de dominio de Internet [53] que clasifica los nombres de dominio bajo ".es" en regulares y especiales, siendo los primeros aquéllos que se asignan conforme a las reglas establecidas en el Plan y los especiales los que pueden ser asignados por la Entidad Pública Empresarial Red.es sin sujeción a las reglas establecidas en el referido Plan cuando concurra un notable interés público para ello.

Los nombres de dominio de segundo nivel bajo el ".es" deben cumplir las normas establecidas en el Capítulo segundo del Plan en el que se recogen las reglas de legitimación para la solicitud de estos nombres de dominio, los requisitos de asignación, las normas de derivación, las prohibiciones y la necesidad de coordinación con el Registro Mercantil Central, la Oficina Española de Patentes y Marcas, los demás registros públicos nacionales y la Oficina de Armonización del Mercado Interior para la asignación de los nombres de dominio de segundo nivel.

Entre las principales novedades que introduce el Plan Nacional destacamos la creación de los nombres de dominio de tercer nivel, esto es, la posibilidad de solicitar el registro de un dominio bajo los indicativos que se recogen en la tabla que examinamos a continuación, los cuales podrán ser solicitados por las personas en ella indicada.

[52] Tal y como venimos señalando, el Ministerio de Ciencia y Tecnología ha pasado a denominarse Ministerio de Industria, Turismo y Comercio. En este sentido, las referencias que se hagan a lo largo de este capítulo al Ministerio de Ciencia y Tecnología han de entenderse realizadas al Ministerio de Industria, Turismo y Comercio.

[53] Plan Nacional de nombres de dominio de Internet bajo el código país correspondiente a España (".es") aprobado por Orden CTE/662/2003, de 18 de marzo, que ha venido a derogar la Orden del Ministerio de Fomento de 21 de marzo de 2000, que regulaba el sistema de asignación de nombres de dominio de Internet bajo el código país correspondiente a España ".es", que es la que hasta el momento regulaba esta materia, con las modificaciones que le realizó la Orden de 12 de julio de 2001 del Ministerio de Ciencia y Tecnología con el objeto de subsanar determinados errores que dificultaban su aplicación, para que pudiese subsistir en tanto se aprobaba el Plan Nacional de nombres de dominio.

NOMBRES DE DOMINIO DE TERCER NIVEL

Nombres de dominio	Legitimación
.com.es	Personas físicas o jurídicas y las entidades sin personalidad que tengan intereses o mantengan vínculos con España.
.nom.es	Las personas físicas que tengan intereses o mantengan vínculos con España.
.org.es	Las entidades, instituciones o colectivos con o sin personalidad jurídica y sin ánimo de lucro que tengan intereses o mantengan vínculos con España.
.gob.es	Las Administraciones Públicas españolas y las entidades de Derecho público de ella dependientes, así como cualquiera de sus dependencias, órganos o unidades.
.edu.es	Las entidades, instituciones o colectivos con o sin personalidad jurídica, que gocen de reconocimiento oficial y realicen funciones o actividades relacionadas con la enseñanza o la investigación en España.

Como reglas comunes a los nombres de dominio de segundo y de tercer nivel se establecen las referentes a los derechos y obligaciones que debe cumplir el que solicita la asignación de un nombre de dominio. Así:

1. Está obligado a facilitar sus datos identificativos siendo responsable de su veracidad y exactitud.
2. Debe respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres de dominio bajo el ".es".
3. Mantendrá informada a la Autoridad de asignación de todas las modificaciones que se produzcan en los datos asociados al registro del nombre de dominio.
4. Como derechos destacamos el de la utilización del nombre de dominio, el derecho a la continuidad y calidad del servicio que presta la autoridad de asignación.

El Plan Nacional establece entre las normas comunes a los nombres de segundo y de tercer nivel las reglas de sintaxis que éstos deben cumplir:

- Los únicos caracteres válidos son las letras de las lenguas españolas, los dígitos "0" a "9" y el guión (-)
- El primero y el último carácter del dominio no puede ser el guión
- Los cuatro primeros caracteres del nombre de dominio no podrán ser "xn - -"
- La longitud mínima admitida para un dominio de segundo nivel es de tres caracteres y de dos caracteres para un dominio de tercer nivel
- La longitud máxima para un dominio de segundo y de tercer nivel es de sesenta y tres caracteres

Además de los nombres de dominio que hemos analizado, la Unión Europea a través del Reglamento (CE) nº 733/2002 del Parlamento Europeo y del Consejo, de 22 de abril, ha aprobado la creación del dominio de primer nivel ".eu". Se trata de un dominio de código de país, que se aplicará con independencia de los dominios nacionales de los Estados miembros de la Unión Europea.

2.2. ¿Cómo adquirir un nombre de dominio?

El derecho a usar un nombre de dominio con carácter exclusivo se adquiere mediante su registro. Son varios los pasos que deben darse en este sentido y varían según el nombre de dominio que se quiera registrar sea uno genérico o de código país.

El sistema de registro de un nombre de dominio está estructurado sobre la base de un órgano central que es la Corporación Internacional de Asignación de Nombres y Números de Internet, en adelante la ICANN, y un sistema de bases de datos centralizada que permite que un mismo nombre de dominio no pueda ser registrado por dos personas a la vez.

Teniendo esta estructura presente, otra cuestión a tener en cuenta es que son muchos los sujetos que intervienen en el registro de un nombre de dominio y se hace preciso conocerlos para poder acudir al que sea necesario en cada momento.

Los nombres de dominio que se registran son los de segundo y tercer nivel bajo los nombres de dominio de primer nivel, en un caso, sean estos genéricos como el ".com", ".net", ".org" o de código país como el ".es" y bajo los nombres de dominio de primer y segundo nivel como los de ".com.es", ".nom.es", ".gob.es", ".edu.es" y ".org.es".

Por poner un ejemplo, en el caso de "cscamaras.es" lo que registramos es "cscamaras" que es el dominio que nosotros hemos elegido y el que tenemos interés en registrar para nuestro tráfico mercantil *on line.* Y en el caso de www.midominio.com.es lo que registramos también es "midominio" dado que el ".com.es" es el indicativo de código país bajo el que lo registramos.

a. Sujetos intervinientes

Para conocer el procedimiento de registro de un nombre de dominio hay que conocer a los sujetos intervinientes en el mismo, que son:

1. **Corporación Internacional de Asignación de Nombres y Números de Internet (ICANN),** que se encarga de establecer las cláusulas y condiciones en relación con una controversia que surja sobre el registro y utilización de un nombre de dominio de Internet registrado. Lleva un control de todos los nombres de dominio que se registran de modo que cada vez que se registra un nombre de dominio se realiza una cesión de los datos del registrador a la ICANN.
2. **Entidades de registro** o entidades administradoras y responsables del registro de nombres de dominio. Cada nombre de dominio genérico y de código país tiene una entidad encargada de su registro a nivel mundial. Siendo Internet una red universal y pudiendo solicitarse el registro de un mismo nombre de dominio desde cualquier parte del mundo, se ve necesaria la existencia de esta figura que centralice el registro de uno o varios nombres de dominio permitiendo de este modo que el sistema de los nombres de dominio y su característica de identificadores comerciales en Internet pueda ser efectivo.

   Las Entidades encargadas del registro de los nombres de dominio genéricos son las que se reflejan en la tabla que sigue:

NombrFe de dominio	Entidad registradora
".com", ".net"	Verisign Global Registry Services
".org"	Public Interest Registry
".biz"	NeuLevel Inc.
".info"	Afilias Ltd.
".pro"	RegistryPro Ltd.
".name"	Global Name Registry LTD.
".coop"	DotCooperation LLC.
".aero"	Société Internationale de Télécommunications Aéronautiques (SITA)
".museum"	Museum Domain Management Association (MDMA)

En lo que a los nombres de código país se refiere también ocurre que hay una Entidad encargada del registro del dominio correspondiente. En el caso de España, el dominio ".es", la autoridad encargada de la asignación de nombres de dominio bajo el ".es" es la Entidad Pública Empresarial Red.es, que lo hace a través de su departamento ESNIC.

Nombre de dominio	Entidad registradora
".es"	Red.es: www.red.es Esnic: www.nic.es

En este caso particular encontramos otras figuras que intervienen en el registro de un nombre de dominio con carácter excepcional, y en algunos casos por nueva creación del Plan Nacional de nombres de dominio, que son los **agentes registradores,** que actuando en régimen de libre competencia asesoran a los usuarios, tramitan sus solicitudes y actúan ante la autoridad de asignación para la consecución de la asignación de nombres de dominio y el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información que asesora al Gobierno sobre la gestión del dominio ".es".

3. **Entidades acreditadas por la ICANN:** son empresas proveedoras de servicios de registro y mantenimiento de nombres de dominio acreditadas por la ICANN. Si esta corporación es el órgano de mayor jerarquía en lo que a la asignación de nombres y números de Internet se refiere, es fácil comprender que las empresas que colaboren en la tarea de hacer posible el registro de los nombres de dominio deban cumplir el requisito de ser acreditadas por ella. Así en su página web, www.icann.org, en la columna de la izquierda donde dice *Registrars* podemos acceder a una tabla de las entidades acreditadas por orden alfabético y con indicación del país para el que están acreditadas y la relación de los nombres de dominio cuyo registro pueden tramitar.

   En concreto en España encontramos las siguientes empresas proveedoras de servicios:

EMPRESAS PROVEEDORAS DE SERVICIOS EN ESPAÑA
Allglobalnames: www.cyberegistro.com
Arsys: www.soloregistros.com; www.arsys.es
Nominalia Internet, S.L.: www.nominalia.com
Interdomain: www.interdomain.org
Entorno Digital, S.A.: www.entorno.es

Esto respecto a los nombres de dominio genéricos, en cuanto a los nombres de dominio de código país, ocurre igual, es una entidad registradora la que se encarga de administrar la gestión de los nombres de dominio bajo el código país correspondiente.

En España, como ya hemos comentado anteriormente, es la Entidad Pública Empresarial Red.es la que centraliza el registro del nombre de dominio de código país que corresponde a España (".es") y como empresas proveedoras de servicios en lo que al registro del dominio ".es" se refiere podemos consultar la lista de Registradores que hay en la dirección de Internet http://www.nic.es/agentes/listado.html.

4. **Solicitante de un nombre de dominio:** Para solicitar un nombre de dominio no se necesitan otros requisitos que los de aquellos que exija el nombre de dominio que se solicite, es decir, según el nombre de dominio sea de libre acceso o sea de acceso restringido a un grupo de personas determinados, como por ejemplo ocurre con el dominio ".edu" que está reservado para centros educativos y universidades.
5. **Otros: persona de contacto, persona de facturación:** Cuando se solicita el registro de un nombre de dominio se piden al que lo registra un conjunto de datos que son de contacto para tenerlos en la base de datos "Whois", a la que nos referiremos después, y ponerlos así a disposición del público para facilitar su contacto. Además se solicitan datos para proceder a la facturación del precio que el tener un nombre de dominio registrado devenga.

b. Elección del nombre de dominio

Cuando una empresa va a proceder a elegir el que será su signo identificativo en el tráfico comercial *on line,* debe tener muy presente que sus servicios y productos se van a relacionar directamente con él en el ámbito del comercio electrónico, y por tanto la decisión del que vaya a ser su nombre de dominio no es una decisión trivial sino que en ella va en juego la identificación de nuestro trabajo.

Generalmente las empresas prefieren elegir como identificativo en la red el mismo signo que les identifica en el comercio *off line,* de ahí que surjan los problemas que el nombre de dominio presenta en relación con las marcas u otros identificativos comerciales.

Cada entidad registradora puede dictar las normas de regulación del nombre de dominio que tiene asignado, si bien, la *Internet Engineering Task Force* (IETF), a través de su Recomendación RFC-1034, estableció las normas de sintaxis básicas de los nombres de dominio genéricos por las que se reconocieron como posibles caracteres válidos de los nombres de dominio las letras del alfabeto inglés, los dígitos del 0 al 9 y guión "-". Han de tener una longitud máxima de 63 caracteres, comenzar y acabar por letra del alfabeto inglés o dígito del 0 al 9 y sólo pueden estar formados interiormente por letras del alfabeto inglés, dígitos del 0 al 9 y guión "-".

Siguiendo estas reglas podría ser un nombre de dominio válido el de *c-a-m-a-r-a-s.org* pero no el de *-camaras-.org*.

Han resultado polémicas las reglas por las que se establece que la composición de los nombres de dominio sólo puede realizarse con caracteres del alfabeto inglés, en relación con las lenguas que contienen caracteres diferentes a los de este alfabeto. Si consideramos de un alto valor comercial el hecho de que una empresa pueda solicitar como nombre de dominio la denominación por la que es comúnmente conocida, ¿qué ocurre cuando esa denominación está formada por caracteres como la "ñ", la "ç", vocales acentuadas, y con los alfabetos japoneses, coreanos, árabes, etc., ...?

Las razones que motivan la necesidad de un reconocimiento general de los caracteres distintos a los del alfabeto inglés son múltiples ya se contemplen desde el punto de vista del usuario o desde el del empresario, siendo de gran valor tanto para darse a conocer como empresario como para el usuario que busca el servicio o producto que se ofrece.

Un importante paso en este sentido lo ha dado el Plan Nacional de nombres de dominio al reconocer en sus normas de sintaxis, aplicables a los nombres de dominio de segundo y de tercer nivel bajo el indicativo ".es" los caracteres de las lenguas españolas.

c. Registro de nombre de dominio

Realizada la elección del nombre de dominio se procederá a intentar su registro. Cuando se quiera registrar un nombre de dominio genérico, habrá de acudir a una de las entidades acreditadas por la ICANN para poder proceder al registro de los nombres de dominio que se soliciten. Una vez elegida la entidad de registro, los pasos a realizar son los siguientes:

1. Comprobar que el nombre de dominio que se solicita está libre. Para ello se consultará la base de datos "Whois", que es la base de datos que contiene una relación entre los nombres de dominio y sus titulares, identificando a estos a través de su nombre, dirección y datos la persona que sea el contacto administrativo, entre otros.
2. Dirigirse a una de las entidades acreditadas por la ICANN.
3. Aceptar las condiciones legales para registrar un nombre de dominio genérico.
4. Solicitarlo y esperar respuesta de la entidad registradora.

Por su parte, los nombres de dominio de código país y en concreto el que corresponde a España, el ".es", debe registrarse ante la entidad registradora acreditada por la ICANN, que como hemos señalado es Red.es. El registro de un nombre de dominio bajo el ".es" implica una primera comprobación de las normas establecidas en el Plan Nacional, anteriormente referidas y a continuación se procede a enviar el Formulario de Solicitud Electrónica de asignación de un nombre de dominio, que se encuentra en la página web de la entidad registradora.

En virtud del registro del nombre de dominio, la persona que aparece como titular del mismo adquiere únicamente el derecho a utilizar dicho nombre de dominio a efectos de direccionamiento en el sistema de nombres de dominio de Internet durante el periodo determinado por el Registrador Competente y asume todas las obligaciones que se desprenden a lo largo de este contrato así como las indicaciones de las normas establecidas tanto por el registrador competente, como por la entidad registradora correspondiente, como por la ICANN en esta materia.

Hay que tener en cuenta que en el registro de un nombre de dominio rige el principio de que el primero que lo solicita es quien lo obtiene *("first come, first served").*

2.3. Recuperación de un nombre de dominio

En el caso de conflictos que tengan por objeto el registro de nombres de dominio, como alternativa a la solución judicial de controversias, existe una Política Uniforme de solución de controversias en materia de nombres de dominio, aprobada por la ICANN el 26 de agosto de 1999 y un Reglamento de la Política Uniforme de solución de controversias en materia de nombres de dominio, aprobado el 24 de octubre de 1999.

La Política Uniforme se aplica a los prestadores de servicios de registro de nombres de dominio que la hayan adoptado y a los prestadores de servicios de solución de controversias en la materia acreditados por la ICANN. Sin embargo, algunos nombres de dominio poseen sus propias políticas de resolución de conflictos.

La Política Uniforme y su Reglamento se aplican a las controversias que se susciten entre un tercero y el titular de un nombre de dominio, en las que el demandado se somete obligatoriamente a este procedimiento administrativo y el demandante tiene que probar que:

– El nombre de dominio que motive la demanda sea idéntico o similar hasta el punto de crear confusión con una marca sobre la que el demandante tiene derechos

– No existen derechos o intereses legítimos sobre el nombre de dominio por parte del demandado

– El registro y la posesión del nombre de dominio sean de mala fe

El prestador de servicios de solución de conflictos en materia de nombres de dominio que más controversias solventa conforme a esta Política es el Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual (OMPI) en Ginebra.

A continuación puede observarse el esquema de procedimiento ante la OMPI:

ESQUEMA DE PROCEDIMIENTO

Presentación de la demanda ante el centro de Mediación y Arbitraje (incluida la portada de transmisión) (remisión por correo-e y envío por correo ordinario de original y cuatro copias por servicio de mensajería)	Envío de una copia de la demanda al: ☐ demandado ☐ registrador
Efectuar el pago de las tasas del Centro	
Examen por el Centro del cumplimiento de los requisitos formales de la demanda en el plazo de cinco días naturales a partir de la presentación de la demandada	
Si cumple los requisitos formales, remisión al demandado en el plazo de tres días naturales a partir de la recepción de las tasas. Fecha de comienzo del procedimiento administrativo	
Plazo de veinte días en el que el demandado deberá contestar	
Si las partes no han optado por un grupo de expertos de tres miembros, el Centro nombrará, en un plazo de cinco días naturales a la recepción del escrito o una vez transcurrido dicho período, un único panelista	
Una vez nombrado el panelista, se notificará a las partes la fecha límite en la que, sin que existan circunstancias excepcionales, se remitirá al Centro la resolución sobre la controverisa	

En especial la resolución del caso "davara.net"

En este apartado se busca ilustrar la recuperación del nombre de dominio "davara.net" por un especialista del Derecho de las TIC, el profesor D. Miguel Ángel Davara Rodríguez, Presidente de la Firma Davara & Davara, tras ver suplantada su identidad en Internet, sufriendo un grave perjuicio a su reputación, supuesto de hecho pionero en las controversias de resolución de conflictos de nombres de dominio. El caso fue resuelto por la OMPI a favor de la Firma Davara & Davara Asesores Jurídicos, demandante en el conflicto.

La recuperación del nombre de dominio "davara.net" es el primer caso en que se usurpa la identidad de un profesional en España y éste recupera su dominio.

Los hechos se remontan al verano de 2001, cuando una persona que decía llamarse Luis Davara, con nacionalidad supuestamente venezolana y afincado en México, registró el dominio objeto de controversia a través de un registrador situado en París (Francia) y creó una página web que pretendía ser el sitio web de la Firma Davara & Davara Asesores Jurídicos, en la que todos los links que se incluían en

la misma dirigían siempre a la única página que se encontraba bajo el dominio "davara.net", además de incluir algunas secciones bajo nombres tales como "Cursos y Seminarios. Máster del prof. Davara" o "Sección destacada: el profesor Davara responde", aludiendo de nuevo a la supuesta presencia y atención del Presidente de la Firma tras dicha página web, y con clara intención de aprovecharse de la reputación del Prof. Davara.

Lo anterior supuso que se iniciara un procedimiento ante la OMPI[54] con el fin de recuperar el nombre de dominio en cuestión, siendo las partes del conflicto, por un lado, el demandante, la Firma Davara & Davara Asesores Jurídicos, especializada en Derecho de las Tecnologías de la Información y las Comunicaciones (TIC), fundada y presidida por D. Miguel Ángel Davara Rodríguez, Profesor Ordinario (Catedrático) de la Universidad Pontificia Comillas (ICAI-ICADE), pionero y experto reconocido internacionalmente en Derecho de las TIC. Davara & Davara es una Firma española, titular del nombre de dominio "davara.com", sitio web que contiene información especializada única y exclusivamente en el análisis de las diferentes cuestiones que componen el Derecho de las TIC.

La Firma es asimismo titular del nombre de dominio "davara.org" y de derechos marcarios sobre la marca de comercio DAVARA.ES, registrada en la Oficina Española de Patentes y Marcas, para la clase 42 con destino a "servicios jurídicos".

Por otra parte, el demandado, supuestamente, porque en ningún momento se acreditó su identidad, era Luis Davara, con domicilio en El Mirador 193, Despacho 3. 01310 México, D.F. México.

En relación con la utilización del dominio "davara.net" por el demandado, inicialmente incluyó una página en la que se presentaba como Davara & Davara, intentando beneficiarse no sólo de la imagen de ésta sino también de la actividad profesional y académica del Prof. Davara, al incluir algunos enlaces a secciones tales como "el prof. Davara responde".

Todo ello, por supuesto, constituye una suplantación de la identidad y una explotación de la reputación ajena, incidiendo en cuestiones de competencia al afectar gravemente a la imagen de la Firma y del Prof. Davara. El contenido de esta página inicial fue protocolizado por un notario a petición de Davara & Davara, sirviendo posteriormente como prueba en el procedimiento para la recuperación del nombre de dominio.

Poco tiempo después el demandado cambió el contenido de dicha página por otra en la que se indicaba que se trataba de una página personal, si bien bajo el subdominio "davara.es.org" al que se redireccionaba automáticamente a todo usuario que solicitaba ver la página "davara.net".

Lo anterior debe considerarse, en su caso, sin perjuicio de las infracciones en que haya podido incurrir al registrar dicho nombre de dominio, es decir como fase posterior, o en tal caso paralela, al inicio del procedimiento de recuperación del nombre de dominio ante la OMPI.

La demanda fue presentada ante el Centro de Arbitraje y Mediación de la OMPI mediante el envío de una copia a través de correo electrónico y en soporte papel, original y cuatro copias, mediante Courier a la dirección indicada, así como al registrador del dominio, Gandi, que se encuentra en Francia, y al demandado a la dirección que aparecía en el registro (El Mirador 193, Despacho 3, 01310, México, México, D.F.), siendo dicha dirección inexacta o incompleta, como así hizo constar el servicio Courier (DHL), cuestión que se puso en conocimiento del Centro a través de un escrito complementario, y sin que el demandado, tal y como consta en la Decisión, verificase dicha dirección, proporcionando otra de su supuesta estancia provisional en Venezuela, si bien en la Decisión se hace constar que éste ha alegado ser un estudiante venezolano que cursa estudios de especialización en México D.F.

[54] *Organización Mundial de la Propiedad Intelectual, cuyo Centro de Arbitraje y Mediación es un prestador de servicios de solución de controversias acreditado por la ICANN.*

Como idioma del procedimiento, dada la nacionalidad y residencia española de la Firma y la teórica residencia en México del demandado, se solicitó el castellano. Asimismo, el demandado contestó sus escritos en castellano, por lo que el Centro aceptó que el idioma del procedimiento fuera éste con base en la tácita aceptación del demandado y en atención a las nacionalidades y domicilios de las partes en países cuya lengua oficial es el castellano.

La resolución depende de la prueba de los tres requisitos exigidos por la Política Uniforme en su art 4 (a) en el que, como ya hemos referido en el apartado referente a la solución extrajudicial de controversias, se exige que se pruebe: i) la identidad o similitud que cree confusión, ii) la ausencia de derechos o un interés legítimo del demandado en el nombre de dominio y, iii) el registro y uso del nombre de dominio con mala fe por el demandado.

En el caso que nos ocupa el panelista señaló lo siguiente:

i) En relación con la identidad o similitud que cree confusión dispone que existe tal entre el dominio “davara.net” y la marca “DAVARA.ES”.

ii) En cuanto a la ausencia de derechos o un interés legítimo del demandado en el nombre de dominio, al no haber acreditado su identidad el demandado ante la solicitud del Centro, concluye el panelista que no tiene derecho o interés legítimo respecto al nombre de dominio “davara.net”.

iii) Respecto del tercer requisito, el registro y uso del nombre de dominio con mala fe por el demandado, el panelista entiende que el demandado ha registrado primero y usado luego el nombre de dominio en disputa para interferir en la actividad en línea del demandante y causar así molestia a su propietario y director, constituyendo así una conducta de mala fe.

Después de analizar todo esto, el panelista concluyó en resolución D2002-0220, de 10 de junio de 2002, que el nombre de dominio “davara.net” fuese transferido a Davara & Davara, Asesores Jurídicos. El texto completo de la decisión se encuentra disponible en la dirección de Internet http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0220.html.

capítulo cuarto

Otros aspectos de la Sociedad de la Información

1. ADMINISTRACIÓN ELECTRÓNICA

Cuando entramos a analizar la repercusión que las Nuevas Tecnologías están representando en la Administración pública y en las empresas nos encontramos con que son muchos los recursos que las TIC ofrecen a este ámbito de la sociedad. Procederemos brevemente a señalar algunos de ellos, dado que la extensión que puede alcanzar el análisis de esta materia es muy grande comparada con el espacio reducido que representa en la obra que nos ocupa.

a. Planes de actuación

El impulso del uso de las Nuevas Tecnologías en este ámbito ha venido respaldado por planes e iniciativas europeas, en virtud de los que correlativamente el Gobierno español ha procurado ir marcando objetivos a conseguir como son posibilitar el uso de Internet y de la informática en todos los rincones de España, fomentar la telemedicina, y prestar servicios de la administración a través de la Red, entre otros.

Así, inicialmente y para conocer los antecedentes de los planes de acción actuales (eEuropa 2005 y España.es), el Plan de Acción eEurope 2002 se reflejó en la iniciativa española Plan de Acción Info XXI que preveía como acciones prioritarias la introducción de la Sociedad de la Información en los distintos sectores de la sociedad.

Entre sus objetivos principales destacaba el buscar implantar la Sociedad de la Información en España para ciudadanos y empresas y la participación de éstos en su construcción. Para lo que se entendía que se podían aprovechar las oportunidades que se ofrecen para aumentar la cohesión social, mejorar la calidad de vida y la calidad de trabajo, así como acelerar el crecimiento económico.

Esta iniciativa ha tenido otras como el Plan de Acción eEurope 2002 y posteriormente el del 2005 como medidas elaboradas a nivel comunitario para el desarrollo de la Sociedad de la Información. En este Plan de Acción se prevén unos objetivos a alcanzar a través de un conjunto de medidas legislativas, económicas y sociales. Con la adopción de dicho Plan, la Unión Europea busca una posición de ventaja en la utilización de las TIC en la sociedad, de manera que todos los sectores, público y privado, y los ciudadanos, puedan beneficiarse de las mismas.

Cabe señalar que el Plan de Acción concreta unas medidas que tienen por objeto desarrollar determinados aspectos en cada uno de los ámbitos en los que se aplican las TIC, indicando en su caso los plazos en los que deberán adoptarse las medidas

concretas y los sujetos que deberán aplicar estas medidas, ya sean la Comisión Europea, los Estados miembros o el sector privado, entre otros.

En concreto y en lo que al marco dinámico establecido para los negocios electrónicos, se preveía la supresión de los obstáculos que impiden a las empresas la realización de negocios electrónicos, el establecimiento de una red europea de apoyo a los negocios electrónicos para PYMES y una capacitación digital, en Europa, mediante un análisis de la oferta y la demanda. Otra posibilidad que se ofrece es a las empresas europeas las funcionalidades vinculadas al nombre de dominio ".eu".

b. Programa España.es

El Programa de actuaciones para el desarrollo de la Sociedad de la Información en España, conocido como "España.es", destaca, en lo que a las PYMES se refiere que *la competitividad de la economía nacional, la mejora de la productividad y la creación de puestos de trabajo, está estrechamente relacionado con la capacidad de nuestras PYMES para aprovechar los beneficios de las Tecnologías de la Información tanto en sus procesos productivos como en la mejora de sus sistemas de aprovisionamiento y comercialización de sus productos y servicios.*

Aunque el desarrollo de las TIC en el ámbito empresarial varía de unos sectores a otros, el Programa España.es quiere poner de manifiesto la necesidad de impulsar estas Nuevas Tecnologías de manera que lleguen a todos los sectores de actividad.

Así por ejemplo, recoge el Programa como cifras la de una conectividad del 90% en los sectores de los Servicios Financieros, Informática e I+D (investigación y desarrollo), mientras que el Comercio Minorista y Hostelería se queda por debajo del 45%. Entre ambos se sitúa el sector del Transporte y Comunicación con un 74%. De la misma manera, casi un 60% de las PYMES de 1 a 9 empleados tienen acceso a Internet, mientras que el porcentaje para PYMES del siguiente tramo por tamaño de empresa de 10 a 49, sube hasta el 86%, sin olvidar que prácticamente todas las empresas de más de 100 empleados están conectadas.

Como resultado de la experiencia acumulada en los diferentes programas antes mencionados, así como de análisis realizados, se han identificado cinco grandes necesidades por resolver:

1. Por una parte la necesidad de identificar servicios y contenidos específicos de alto valor añadido que sean percibidos por las empresas como un beneficio directo para su actividad. En este ámbito se ha detectado que los servicios de carácter horizontal útiles para todas las empresas (conectividad, servicios TIC básicos, soluciones ASP para contabilidad o gestión, páginas web, e-mail, …) no representan por sí mismos un valor añadido suficiente para las empresas que justifiquen la realización de las inversiones correspondientes para su utilización.
2. Servicios horizontales que facilite a las empresas de una manera sencilla e inmediata la implantación de las soluciones sectoriales antes señaladas y que también cubra la demanda de este tipo de necesidades, desde la conectividad básica de las PYMES, pasando por el desarrollo de aplicaciones horizontales innovadoras dentro de la Sociedad de la Información (ASPs, contabilidad, gestión de Recursos Humanos, etc.).

   Se plantea por otra parte poner en marcha un programa de promoción de "sellos de garantía" de comercio seguro por parte de organizaciones independientes; se trata de promover la creación de entidades que certifiquen la realización de comercio electrónico seguro, tratando de inducir confianza entre las PYMES.
3. Especialmente en el caso de la creación electrónica de empresas, licencias, la gestión de trámites ante la Seguridad Social, así como en la contratación con Administraciones Públicas. La Administración será un "prescriptor" más de la PYME en lo que a las TIC respecta y se prestará una especial atención al desarrollo de servicios que sean especialmente útiles para mejorar las relaciones

de estas empresas con la Administración facilitando el cumplimiento de sus obligaciones, la solicitud de ayudas, la obtención de permisos y licencias, etc.

4. Elaboración de una legislación específica que fomente y apoye el uso de las Nuevas Tecnologías a través de la consolidación de la e-confianza en el ámbito de las PYMES, por medio de medidas como la certificación electrónica, el desarrollo de servicios CERT o de medios de pago electrónicos –por ejemplo: dinero electrónico, títulos cambiarios electrónicos, etc, igualmente se promulgará la normativa reglamentaria llamada a favorecer el desarrollo del comercio electrónico.
5. Asesoramiento y la formación: se proponen en este sentido Programa de asesores TIC/becarios con Universidades y Formación Profesional (FP), líneas de cooperación con Organizaciones y Asociaciones empresariales en los distintos ámbitos sectoriales y territoriales, favorecer el diagnóstico y el asesoramiento TIC a PYMES, entre otros, a través de la Fundación Navega.es. En lo que respecta a la comunicación de las condiciones que incentivan a las empresas a incorporar las TIC, se proponen medidas dirigidas a informar sobre los paquetes de conectividad, los servicios específicos y/o horizontales, la formación y asesoría así como las ventajas y beneficios fiscales existentes en este ámbito.

Los objetivos del programa España.es son principalmente:

I. ***Administración.es***: impulsar decididamente la Administración Electrónica.

II. ***Educación.es***: del "aula de informática" a la "informática en el aula", integrando las Nuevas Tecnologías como herramienta habitual en el proceso de enseñanza/aprendizaje. Actuación que se extenderá al periodo 2004-2007.

III. ***PYMES.es***: incorporación de las PYMES a la Sociedad de la Información de una manera coordinada e integrada, desarrollar e implantar soluciones y servicios, y formar a las PYMES menos integradas en la Sociedad de la Información.

IV. ***Navega.es***: accesibilidad de todos los ciudadanos a la Sociedad de la Información, acercando la Sociedad de la Información a todos aquellos colectivos menos integrados a través de dotación de infraestructuras y plan de formación. Instalando 2000 nuevos centros de acceso público a Internet en áreas rurales, con banda ancha.

V. ***Contenidos.es***: crear contenidos digitales de calidad, ofreciendo a la sociedad contenidos de titularidad pública y promover un uso más seguro de Internet.

VI. ***Comunicación.es***: comunicar a toda la sociedad las ventajas de la Sociedad de la Información, creando una marca para todas las actuaciones, y con una campaña "paraguas" y campañas específicas. Este objetivo es responsabilidad del Ministerio de Industria, Turismo y Comercio [55] que ya ha puesto en marcha la campaña "Todos.es" que tiene por objeto acercar la Sociedad de la Información a los ciudadanos.

c. Administración.es

Entre los servicios que aparecen ofrecidos en la página web de la Administración electrónica (www.administracion.es) en el apartado de la Administración en Internet vamos a destacar aquéllos que entendemos pueden ser de mayor interés en el ámbito que desarrollamos este trabajo cual es el empresarial, de este modo, encontramos específicamente entre los servicios ofrecidos a las empresas:

- Entre otros servicios que se ofrecen encontramos mucha presencia estática de la administración ofreciendo numerosa información de interés para los ciudadanos como por ejemplo refe-

[55] *Tal y como venimos señalando, el Ministerio de Ciencia y Tecnología ha pasado a denominarse Ministerio de Industria, Turismo y Comercio. En este sentido, las referencias que se hagan a lo largo de este capítulo al Ministerio de Ciencia y Tecnología han de entenderse realizadas al Ministerio de Industria, Turismo y Comercio.*

rente a su documentación personal como DNI y pasaporte, información relativa a los centros sanitarios existentes y la posibilidad de realizar determinadas consultas.

- En el ámbito de la Administración de Justicia además de la función informadora ofrece la Administración la posibilidad de realizar algunos trámites como son las solicitudes de certificados on line de nacimiento, matrimonio y defunción. O en los Registros de la Propiedad la posibilidad de solicitar información sobre datos inscritos en los Registros así como la información interactiva que se ofrece desde los Registros Mercantiles.
- En el ámbito de la Administración Tributaria electrónica, la naturaleza trasnacional de Internet pone en cuestión no el régimen jurídico de los impuestos sobre el comercio internacional, sino sobre todo el control del cumplimiento de las normas existentes hasta el momento en el Derecho Internacional Tributario.

Las situaciones tradicionales de fraude fiscal (declaraciones, documentos y facturas falsos...) se agravan con el perfeccionamiento electrónico de las transacciones. La problemática de la generación y control de documentos de manera electrónica es otro de los objetivos de las legislaciones en materia tributaria en relación con el comercio electrónico. En este sentido, nos remitimos al capítulo de fiscalidad electrónica.

2. VENTANILLA ÚNICA EMPRESARIAL (VUE) DE LAS CÁMARAS DE COMERCIO

Se trata de un instrumento de apoyo a los emprendedores en la creación de nuevas empresas, mediante la prestación de servicios integrados de tramitación y asesoramiento empresarial.

La Ventanilla Única Empresarial es un programa de simplificación administrativa de las condiciones para la creación de empresas impulsado a iniciativa conjunta de todas las Administraciones Públicas (Administración General del Estado, Comunidades Autónomas, Administraciones Locales) y las Cámaras de Comercio.

La Ventanilla pone a disposición de los emprendedores:

- Una extensa red de Centros presenciales de tramitación y de asesoramiento integral al emprendedor (31 hasta la fecha).
- El Portal Ventanilla Única Empresarial Virtual (http://www.vue.es), que ofrece información general sobre creación de empresas, una herramienta de orientación personalizada y tutorizada sobre los trámites de cada proyecto empresarial, así como un sistema de seguimiento individualizado de los trámites que se realicen para la puesta en marcha de una empresa.

Entre sus objetivos principales cabe destacar:

1. Facilitar la tramitación, acercando la Administración al ciudadano y haciendo posible que en un solo espacio físico se puedan realizar todos los trámites necesarios para la puesta en marcha de una empresa cuya competencia corresponde a: Hacienda, la Tesorería General de la Seguridad Social, la Comunidad Autónoma y el Ayuntamiento.
2. Informar y orientar al emprendedor ofreciéndole un asesoramiento integral en los diversos aspectos que comporta la creación de una empresa: sobre los trámites necesarios para la constitución de empresas, sobre las posibles formas jurídicas, los medios de financiación, las ayudas y subvenciones públicas para la creación de empresas y el autoempleo, la viabilidad económica y empresarial del proyecto, etc.

3. PUBLICIDAD EN INTERNET

3.1. Generalidades

Internet se está configurando como un medio idóneo para realizar publicidad, motivado por el aumento del número de usuarios que aparecen como potenciales targets u objetivos para estos medios publicitarios pudiéndose además, por las especiales características de la red, diferenciar claramente las necesidades de cada cliente potencial.

El origen del uso de Internet como medio de publicidad se encuentra en la necesidad que se planteaba a los que se creaban una página web de financiar ésta mediante la inclusión de publicidad en ella.

Las características de la publicidad que utiliza Internet como medio de comunicación son diferentes, en parte, a las de los medios convencionales porque los anuncios, generalmente a través de banners, no se contratan por tiempo, sino, por ejemplo, por un número de impresiones determinado o de click through, suponiendo así que la tarificación por Internet es más ajustada a la realidad de su eficiencia.

Las posibilidades que ofrece Internet como medio de publicidad están todavía sin explotar en gran medida, y, en nuestra opinión, será necesaria la presencia de nuevos agentes y profesionales en la materia que fomenten el correcto uso y desarrollo de la publicidad por este medio. Entre los agentes que participan en el mercado publicitario podemos destacar las empresas de investigación, encargadas de llevar el control de la efectividad de Internet asesorando a las empresas que piensan en Internet como el medio para realizar su campaña publicitaria. En segundo lugar las agencias de publicidad especializadas en marketing on line, las promotoras publicitarias en Internet, las agencias de publicidad o las centrales de planificación de medios de Internet.

Cada vez más los usuarios de la red buscan una publicidad que contenga un servicio de valor añadido a la información que se está visualizando y sobre la que se está interesado.

La ventaja que ofrece Internet es posibilitar que la empresa pueda realizar acciones de comunicación y de promoción en la red al mismo tiempo que puede realizar transacciones comerciales, es decir, se puede conseguir que un cliente conozca el producto, se informe sobre él y lo adquiera al mismo tiempo sin necesidad de esperar a otro momento o tener que desplazarse al punto de venta.

Las ventajas de esta realidad son múltiples, teniendo en cuenta que la eficacia de una campaña publicitaria o de un solo anuncio se ve disminuida con el paso del tiempo, por lo que si somos capaces de asegurarnos la venta del producto en el mismo momento que la campaña publicitaria está surtiendo efecto, tendremos muchas más posibilidades de ventas. Por otro lado la comodidad que representa para los clientes el poder realizar dos acciones en un mismo acto hará que se incrementen las posibilidades de que adquieran nuestro producto. Desde el punto de vista del empresario, esta simplificación de trámites hace que se pueda comprobar la eficacia de la campaña al tiempo que se realiza. Por último cabe señalar la forma interactiva de la comunicación entre el cliente y la empresa, de forma que se facilita la fluidez de la comunicación y el interés que se pueda tener.

Una campaña publicitaria *on line* la podemos considerar como el conjunto de acciones publicitarias realizadas a través de Internet en un periodo de tiempo determinado sin pausas, y referida a un mismo producto.

3.2. Herramientas de publicidad

Algunas de las principales herramientas de publicidad en las páginas o sitios web son:

- ***Banners:*** son pancartas interactivas y panorámicas que, en su versión más popular, se colocan en la parte superior de las páginas web. Se caracterizan por ser un formato publicitario de emplazamiento fijo que en ocasiones se presenta como entrada al sitio web.

No debemos confundir esta herramienta con otras como son los botones que cumpliendo la misma función que los *banners* se caracterizan por su forma cuadrada y su ubicación en un lateral de la página web. De otro lado están los patrocinios que aunque pudiendo considerarse técnicamente como un *banner,* se diferencia de éste en que pertenecen a una marca y tiene una finalidad concreta que es la de dar oficialidad a la página en la que aparece.

La efectividad de los *banners,* como herramienta publicitaria, dependerá en gran medida de su tamaño, de su diseño y de la facilidad y rapidez de carga de la página, cuestiones todas estas que deberán quedar reflejadas en el contrato de publicidad mediante *banners*.

De este modo, respecto del tamaño de un *banner,* éste deberá ser el mínino indispensable que permita contener la información que queremos dar y con las características que deseamos. El tamaño es importante para determinar la velocidad de la página y la posibilidad de que tenga un contenido mayor.

Un segundo factor importante es el del lugar de aparición, dado que las páginas web generalmente no muestran en un primer momento todo su contenido, de modo que cuanto más al principio se encuentre mayor probabilidad de ser visto tienen.

La fijación de las frecuencias es el tercer factor determinante de la efectividad de los *banners,* así cuanto menor sea la frecuencia del mensaje, mayor será el número de recursos de la página que se deberán utilizar.

Por último, señalar que el mensaje del contenido es otro de los factores principales para que el banner cumpla su cometido publicitario, son diversas las formas que puede adoptar y entre ellas podemos señalar, el *Click here,* las preguntas al cliente potencial, las ofertas gratis o los premios o la inclusión de mensajes enigmáticos.

- ***Metatags:*** *son términos específicos que se introducen en un apartado del código fuente de un documento HTML para indicar a los buscadores de Internet cuál es el contenido de la página.*

Supone una forma de clasificar las páginas web analizando el código fuente para adivinar su contenido. Con este análisis se obtiene la ventaja de conocer el contenido de la página sin necesidad de utilizar las palabras convencionales provocando el hecho de que en algunas páginas se repitan conceptos en su código fuente que permitan que las personas interesadas en ellos los puedan encontrar con facilidad.

El principal problema que se plantea es que en ocasiones se introducen términos en el código fuente que no se corresponden con el contenido de la página pero que son muy solicitados por los internautas de modo que podría plantear problemas de publicidad engañosa.

- *Otras herramientas de publicidad de las páginas web son:*
  - ***Links:*** son partes del texto o imágenes, resaltadas en algún color mediante los que haciendo click con el ratón nos conducen a otra página web perteneciente a la persona que ha insertado la publicidad.
  - ***Ventanas pop-up:*** consisten en un mensaje, que se encuentra en una ventana distinta del navegador, que emerge de manera automática al entrar en la página web en la que se insertó.
  - ***Intersticial:*** supone la inserción de un mensaje de transición a la información, es decir, mientras que el usuario espera a que ocurra algo en la pantalla aparece algún producto.

- ***Mini-sites:*** supone un paso posterior a las herramientas anteriormente explicadas, habrá un espacio completo de información publicitaria, al que se accede a través de un enlace y nos muestra con mayor exhaustividad información acerca de un producto.

Una vez analizadas algunas de las principales herramientas de publicidad a través de las páginas web vamos a proceder a examinar brevemente otra forma de publicidad a través de Internet cual es la que se realiza utilizando el correo electrónico.

- ***E-mail:*** suponen el envío de mensajes de correo electrónico a los usuarios conteniendo información publicitaria al respecto. Estos envíos se realizan por las empresas cuyos productos o servicios se anuncian, van dirigidos a destinatarios previamente seleccionados y su contenido es lícito en la mayoría de las ocasiones.
- ***Boletines:*** implican una previa solicitud por parte de los destinatarios para recibir en su correo electrónico boletines que contienen información relacionada con algún tema concreto o genérico o noticias. La inclusión de publicidad en estos boletines tiene por finalidad la financiación de las personas que lo elaboran.
- ***Postales:*** supone un medio de introducir publicidad en las postales de felicitación que facilitan gratuitamente o no determinadas páginas de Internet.
- ***Spam:*** es una forma de publicidad ilícita que consiste en inundar Internet con multitud de copias de un mismo mensaje con la intención de acceder a un gran número de personas a las que de otro modo no se podría acceder.

Entre otros problemas se plantean cuestiones relacionadas con el tratamiento de los datos de carácter personal en los términos que nos referiremos al tratar el tema de la protección de datos.

Otros efectos nocivos que produce el spam es que supone una pérdida de tiempo y de dinero a los destinatarios además de implicar un contenido dudoso dado el anonimato que permite su utilización para los emisores de la publicidad. Por último, es destacable el hecho de que supone un uso de recursos ajenos dado que el remitente de la publicidad invierte menos dinero que el que lo recibe.

3.3. Las cookies

Las *cookies* son ficheros que se introducen en el sistema del usuario con el fin de recopilar información sobre su navegación por Internet. Con carácter general, su utilización no es ilegítima necesariamente, ya que algunas de sus finalidades pueden ser obtener información sobre las preferencias de los usuarios de un sitio web con el fin de estructurar de la manera más adecuada su diseño o verificar la identidad de las partes de una transacción electrónica.

Debe considerarse que en dichos ficheros puede contenerse información personal del usuario, tal como su nombre y apellidos, número de tarjeta de crédito o débito utilizada para el pago de una transacción, u otra información como los apartados de un sitio web a los que accede. En el caso de que haga uso de un ordenador al que puedan acceder terceras personas, ello supone que la privacidad del usuario pueda verse seriamente comprometida si él mismo desconoce que se esté haciendo uso de estos dispositivos.

Los principales problemas que presentan las *cookies* están directamente relacionados con la intimidad de la persona debido a que el usuario no conoce que se han instalado *cookies* en su ordenador. En el caso de que el usuario haya rechazado la admisión de éstas, puede ocurrir que esto provoque que no se le permita navegar por la página web que solicita o que las cookies obtengan igualmente información sobre él.

Así la utilización de *cookies* con dichas finalidades, ya que en otros casos resultaría ilegal, queda sometida a la información y obtención previa del consentimiento del usuario. Si bien, se contempla la posibilidad de que el acceso a determinados contenidos de un sitio web pueda requerir obligatoriamente la aceptación de una cookie.

Actualmente, y como solución tecnológica, algunos navegadores permiten al usuario establecer una configuración que les avise de la utilización de *cookies* por parte del sitio web que visitan, de forma que las mismas sean siempre rechazadas, se le pregunte antes de su aceptación, o puedan introducirse en cualquier caso en su ordenador.

Respecto de la necesidad de informar y obtener el consentimiento previo del usuario, la Directiva 2002/58/CE[56] se remite en este punto a las disposiciones de la Directiva 95/46/CE[57], puesto que su utilización supone un tratamiento de datos de carácter personal, al permitir recabar información.

En cuanto al momento en el que se debe informar al usuario sobre la instalación de este tipo de dispositivos, se señala que podrá hacerse durante la conexión en la que se vaya a proceder a su instalación, permitiendo al usuario la posibilidad de rechazarlo.

Por su parte la LGT ha introducido en la LCE una referencia a las cookies en su artículo 22 cuando en el párrafo 2 dispone que:

> *"Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito (...)".*

Suponen por tanto las *cookies* un instrumento de mucha utilidad para los comerciantes siempre y cuando se utilicen dentro de los límites de la legalidad y del respeto a la intimidad de los usuarios o visitantes. Todo dependerá de la finalidad que se le dé a la información que se recoja.

Entre los buenos usos que se pueden hacer de las cookies están la personalización de las páginas o algunas utilizaciones que se la hayan dado en las tiendas electrónicas como por ejemplo los "carritos".

Como malos usos podemos destacar el seguimiento de visitas realizadas por Internet, el almacenamiento de contraseñas, o los carteles y marketing personalizado.

3.4. Marketing relacional

Entre los condicionantes a tener en cuenta en el marketing a través de Internet uno de los más importantes es el de la relación con los clientes pudiendo resultar esta un tanto impersonal.

Actualmente, muchas entidades dedican gran parte de los recursos a la "fidelización" de los clientes y a la búsqueda de nuevos clientes y para ello eligen dos caminos o bien colocar su publicidad a través de Internet o bien utilizando este medio como vía de comunicación con los clientes más que como medio de colocar su publicidad.

De esta última forma es como se realiza el marketing relacional en el que además de promocionar los productos se busca establecer una relación con los clientes de forma que puedan conocer mejor sus necesidades y puedan ofrecerles productos que se adapten a ello.

---

[56] *Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), publicada en el Diario Oficial serie L, núm. 201, de 31 de julio.*

[57] *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en el Diario Oficial serie L, núm. 281, de 23 de noviembre.*

Los pasos a seguir para realizar este marketing relacional comienzan identificando a los clientes a los que se va a dirigir la campaña. Cuanto más información se tenga de estos clientes y de sus necesidades, más dirigida podrá ser la publicidad.

En un segundo momento y determinados los destinatarios de la campaña de forma muy personal, el paso siguiente es el de determinar el marketing y los productos que se les van a ofrecer para pasar a continuación a colocar la campaña en el medio ofrecido por Internet.

Por último, se procederá al mantenimiento de la relación que se ha establecido con el cliente tratando así de crear un nexo duradero que permita a la entidad presentarse más cercana a los clientes y sufragar así las desventajas que el medio de Internet presenta en cuanto a la impersonalidad de las relaciones proveedor-cliente.

Dos formas de realizar este marketing relacional son el *Customer Relationship Management* (CRM) y el *Permission Marketing.*

En primer lugar, el CRM consiste en la posibilidad de proveer a los empleados de información y procesos para conocer mejor a sus clientes y permite, de un lado, la creación de relaciones individualizadas y de otro una mejora de procesos de venta que identifican y clasifican los clientes en orden de importancia.

Por su parte, el *Permission Marketing* implica el permiso previo de los usuarios para recibir información, de este modo cuanto más interesada esté la gente en recibir información de los productos de una entidad, más posibilidades habrá de conseguir ventas, se busca así más la calidad de los clientes que la cantidad.

4. DELITOS INFORMÁTICOS

Hoy en día cada vez es más patente el alto grado de dependencia de las empresas en la eficacia y seguridad de las modernas Tecnologías de la Información: la mayoría de las transacciones económicas en el ámbito empresarial son administradas por ordenadores. Toda la producción de una compañía frecuentemente depende de su sistema informático de procesamiento de datos, al tiempo que los secretos más valiosos suelen almacenarse electrónicamente.

Esta alta dependencia de las Tecnologías de la Información y las Comunicaciones hace patente el grave daño que los llamados delitos informáticos pueden ocasionar y la importancia que cobra la seguridad con la que han de contar los equipos informáticos y las redes telemáticas con el fin de poner obstáculos y luchar contra dichas conductas delictivas, y la necesidad de tipificar determinadas conductas para que puedan ser positivamente perseguidas y castigadas en el ámbito penal.

Muchas compañías continúan creyendo que sus sistemas y redes informáticas no son los blancos idóneos en un ataque porque no contienen ningún tipo de información que pueda resultar interesante. Esta confianza es errónea dado que los sistemas e infraestructuras de muchas compañías son blancos atractivos por razones que no tienen nada que ver con su contenido. Muchos agresores buscan redes vulnerables pudiendo así explotar los recursos de las mismas, incluyendo las capacidades de procesamiento, el espacio de almacenamiento o el ancho de banda. El deseo del agresor puede meramente consistir en la obtención de un lugar para almacenar su alijo de tarjetas de crédito robadas, pornografía o copias ilegales de software.

De lo dicho se deriva la importancia que para las compañías representan los esfuerzos en la mejora de la seguridad de sus infraestructuras de información, así como desarrollando programas educativos entre sus directivos y empleados sobre la gran vulnerabilidad de la Sociedad de la Información frente a los delitos informáticos, puesto que la mayoría de éstos son causados por la falta de conocimientos de los usuarios.

El delito informático como tal no existe en nuestro derecho, esta expresión se emplea para hacer referencia a aquellas acciones u omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirectamente.

Las características comunes a estas acciones y omisiones que hemos dado en llamar delitos informáticos son:

a. Intangibilidad

El bien jurídico vulnerado por los delitos informáticos es la información y la intangibilidad de la misma es la que ha dificultado la tipificación de estos delitos. Sin embargo, la Sociedad de la Información hace cada vez más necesaria la incorporación de valores inmateriales y de la información como bienes jurídicos de protección, puesto que los daños son graves.

b. Ruptura de la concepción tradicional de tiempo y espacio

La posibilidad de preparar acciones dolosas en perjuicio de otro en tiempo y espacio distantes, ofrecida por el acercamiento en espacio que proporcionan las comunicaciones y por la posibilidad de realizar programas que actúen retardados en el tiempo, aprovechando las funciones del sistema operativo del ordenador que permite activar o desactivar determinadas órdenes a la máquina, posibilitan preparar la acción delictiva mucho antes de que el acto delictivo tenga lugar, pudiendo encontrarse el sujeto activo, en el momento de los hechos, desarrollando una actividad incompatible con la realización del ilícito.

c. Anonimato

El uso de las Nuevas Tecnologías permite ocultar la identidad detrás del uso de los ordenadores, suponiendo ésto un agravante en la persecución de los delincuentes informáticos.

d. Facilidad para borrar las pruebas

Existe un sentido común generalizado que nos indica que ante la escena de un crimen no debemos tocar ni mover nada con el fin de no eliminar posibles huellas digitales u otras pistas para su resolución, sin embargo en el ámbito de los delitos informáticos, ni siquiera los entendidos saben todavía qué evidencias de gran valor en la comisión de delitos informáticos pueden desvanecerse por el mero hecho de encender el ordenador o abrir ficheros del mismo.

Los delitos informáticos pueden diferenciarse, atendiendo a la clasificación que realiza nuestro Código Penal (CP)[58]:

[58] *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el Boletín Oficial del Estado número 281, de 24 de noviembre, y modificada por la Ley Orgánica 15/2003, de 23 de noviembre, publicada en el Boletín Oficial del Estado núm. 283, de 26 de noviembre.*

DELITOS INFORMÁTICOS	TIPIFICACIÓN
Delitos contra la intimidad: Arts. 197 a 201 CP	Descubrimiento y revelación de secretos
Delitos económicos	
Piratería informática (Hacking) Art. 256 CP	Defraudaciones de fluido eléctrico y análogas
Delitos relativos al mercado y los consumidores	
Espionaje informático: Art. 278 CP	Daños
Sabotaje informático: Arts. 248 y 249 CP	Estafa
Fraude informático: Art. 255 CP	Defraudaciones de fluido eléctrico y análogas
Delitos contra la propiedad intelectual:	
Arts. 270 a 272 CP	Delitos contra la propiedad intelectual
*(topografías de productos semiconductores): Art. 273.3 CP	Delitos contra la propiedad industrial
Contenidos ilícitos	
Pornografía infantil: Arts. 186, 187.1 y 189 CP	Delitos contra la libertad sexual
Incitación al odio y a la discriminación: Art. 510 CP	Delitos contra la Constitución
Calumnias e injurias Arts. 205 y ss. CP	Delitos contra el honor
Delitos contra la vida: Art. 346 CP	Estragos
"Guerras informáticas" Art. 265 CP	

En relación con la tipificación de los delitos hecha por el Código Penal, tras las modificaciones introducidas por la Ley Orgánica 15/2003, queremos llamar la atención sobre la polémica suscitada por la redacción del artículo 270 que dice:

> *1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.*
>
> *2. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien intencionadamente exporte o almacene ejemplares de las obras, producciones o ejecuciones a que se refiere el apartado anterior sin la referida autorización. Igualmente incurrirán en la misma pena los que importen intencionadamente estos productos sin dicha autorización, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.*
>
> *3. Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.*

En particular, este último párrafo del artículo 270 supone que cualquiera que tenga una herramienta que permita la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador será reo de este delito contra la propiedad intelectual, lo que ha suscitado críticas y diversas interpretaciones que deberán ser aclaradas mediante la interpretación de este artículo por los Jueces.

Por su parte la Comisión Europea clasifica los delitos informáticos en delitos contra la intimidad, delitos relativos al contenido, referidos a la difusión, principalmente por Internet: de pornografía, declaraciones racistas o violencia, delitos económicos y delitos contra la propiedad intelectual.

Existe en esta materia otra referencia a destacar y es el Convenio del Cibercrimen aprobado el 21 de noviembre de 2001 en Budapest, Convenio impulsado por el Consejo de Europa y en el que han participado también países como Estados Unidos y Japón. Es un Convenio de carácter generalista que deja al arbitrio de los Estados que lo suscriban la concreción de diversos aspectos como es, por ejemplo, la concreción de determinadas categorías delictivas que no obliga a reconocer como tales a los distintos Estados.

Por último en este punto, llamaremos la atención sobre las dificultades que la persecución de los delitos informáticos plantea como son la universalidad y carácter transfronterizo de estos delitos que exige una respuesta rápida y adecuada, requiriendo la existencia de una armonización legislativa y práctica entre los distintos países. Así es importante ser conscientes de que siendo las redes informáticas internacionales, como Internet, medios abiertos que permiten al usuario actuar más allá de las fronteras del Estado, permiten a los delincuentes elegir el país en el que determinadas formas de comportamiento que puedan desarrollarse en un entorno electrónico no se hayan tipificado como delitos.

5. TELETRABAJO

5.1. Introducción

El teletrabajo se concibe como una forma nueva y alternativa de organización del trabajo que implica la necesidad de aprender a trabajar de un modo diferente. Supone una oportunidad para todos, que viene a favorecer, muy especialmente, a los discapacitados con dificultades de movilidad, pero también a otros sectores de la población, como puedan ser las amas de casa, parados, personas que se encuentren en zonas geográficas rurales, etc.

El teletrabajo no deja de ser una forma de relación laboral, en la mayoría de los casos, por lo que para su consideración debemos tener siempre presente la teoría general del derecho laboral y de su norma base, el Estatuto de los Trabajadores (ET)[59], con el fin de poner de manifiesto una vez más que la incorporación de las Tecnologías de la Información y las Comunicaciones al mundo jurídico no supone un cambio en la naturaleza o en el objeto del contrato de trabajo, en este caso, sino un nuevo medio de desempeñar este contrato.

5.2. Concepto

Se puede definir el contrato de trabajo como *aquél que tiene por objeto la libre prestación de servicios personales en régimen de ajeneidad y dependencia, y que son retribuidos por ello bajo el sistema salarial.*

El teletrabajo, sin dejar de reunir las características propias de todo contrato de trabajo implica, la prestación de servicios en que consiste el teletrabajo ha de ser desarrollada en un lugar identificado o identificable que no se corresponda con el del centro de trabajo; un lugar en el que el empresario no esté presente de manera permanente, y que puede incluso haber sido elegido por el trabajador.

[59] *Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores, publicado en el Boletín Oficial del Estado núm. 75, de 29 de marzo (en lo sucesivo, ET o Estatuto de los Trabajadores).*

Supone, además, la necesidad de realizar el trabajo utilizando, de manera significativa y predominante equipos informáticos y telecomunicaciones. Esto es, la utilización de las Nuevas Tecnologías en el desarrollo de la actividad debe ser prevalente, no basta con que la comunicación entre el trabajador y la empresa se realice utilizando medios electrónicos si en el desarrollo de su actividad laboral estos medios no son empleados.

El sometimiento al régimen del teletrabajo es voluntario tanto para el trabajador como para el empresario. El paso al teletrabajo no modifica el estatuto laboral del trabajador, ya que sólo implica modificar la forma en que se realiza el trabajo; luego, el hecho de que el trabajador rechace una oferta de teletrabajo no es razón para resolver el contrato de trabajo ni para cambiar sus condiciones.

5.3. Clases

Atendiendo al lugar en el que se desempeña el trabajo, cabe distinguir:

- Teletrabajo a domicilio: el lugar elegido por el trabajador para el desarrollo de su actividad es su propio domicilio.
- Teletrabajo en telecentro: el lugar de prestación del trabajo es un centro de recursos compartidos con instalaciones informáticas y de telecomunicaciones. Son los centros que se conocen como oficinas satélites.
- Teletrabajo móvil: como su adjetivo indica supone un desplazamiento continuo del trabajador.

El segundo criterio de clasificación del teletrabajo es el del modo de comunicación con la empresa, distinguiéndose entre:

- Teletrabajo *off line:* basado en comunicaciones esporádicas o puntuales entre la empresa y el trabajador.
- Teletrabajo *one way line:* la comunicación se desarrolla en una única dirección, del trabajador con la empresa o de ésta con el trabajador.
- Teletrabajo *on line:* el trabajador desarrolla su actividad con un terminal inserto en una red de comunicaciones electrónicas que permite un diálogo interactivo entre el ordenador central y los diferentes ordenadores, siendo en este caso posible que tanto las directrices como el control por parte de la empresa se lleve a cabo en tiempo real.

Un tercer criterio de clasificación del teletrabajo es el del régimen jurídico aplicable, según la relación sea de trabajo "por cuenta propia" o "por cuenta ajena". En el primer caso, estaremos ante una prestación de servicios o de obra realizada para otro, a través de un contrato mercantil o civil, con plena autonomía y libertad, siendo el teletrabajador un trabajador autónomo (o *freelance).*

Cuando el teletrabajador lo es por cuenta ajena, estamos ante una relación laboral cuyas características principales son la ajeneidad y la dependencia, y que está sujeta al sistema retributivo salarial. La ajeneidad hace referencia a que el trabajador no asume los riesgos derivados del trabajo, pero tampoco posee propiedad sobre sus frutos. Por su parte, la dependencia se refiere a que el empresario es quien asigna y distribuye el trabajo, de manera que el teletrabajador queda sujeto a las instrucciones de la empresa aunque no haya imposición de jornada, horario o trabajo exclusivo.

5.4. Contrato de teletrabajo

El artículo primero del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprobó el texto refundido de la Ley del Estatuto de los Trabajadores, dispone que su ámbito de aplicación es el de *los trabajadores que voluntariamente presten sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario* (art. 1.1 del ET).

A continuación, define la figura del empresario como *toda persona, física o jurídica, o comunidad de bienes que reciba la prestación de servicios de los trabajadores, así como de las personas contratadas para ser cedidas a empresas usuarias por empresas de trabajo temporal legalmente constituidas* (art. 1.2 del ET).

El contrato de teletrabajo es un contrato de trabajo en el que son empleados medios específicos que le atribuyen unas características especiales sin que eso implique un régimen completamente nuevo de la relación laboral.

Al serle, por tanto, de aplicación las reglas generales de los contratos de trabajo, si bien con algunos matices, podemos partir en su análisis del estudio de una relación laboral.

a. Elementos del contrato de teletrabajo

El contrato de trabajo, en términos generales, se caracteriza fundamentalmente por tener los siguientes elementos:

En primer lugar, los elementos **personales,** que son, de un lado, el empresario que contrata y, de otro, el trabajador que es contratado.

En segundo lugar, los elementos **reales,** y éstos son, por un lado, la prestación del trabajador, ya sea de obra o de servicio y, por otro, la contraprestación del empresario que constituye el salario o retribución.

Cuando la prestación del teletrabajador se acerque más a una prestación de obra que de servicio, lo relevante será que el teletrabajador cumpla con su cometido, en calidad y puntualmente, según lo pactado con el empresario.

Por parte del empresario, la contraprestación al servicio pactado, la retribución salarial, es decir que las especialidades que ésta presenta radican en que el salario se ha sujetado tradicionalmente al tiempo de trabajo realizado; así, son estructuras habituales de pago la de destajo y la de tarea:

- ***Destajo:*** el dinero que se percibe es proporcional a cada obra o servicio que se realiza en un determinado periodo de tiempo siendo así que, cuantas más obras se realicen mayor retribución se percibe.
- ***Tarea:*** el salario supone la retribución por un trabajo realizado con independencia del tiempo empleado para el mismo.

La retribución de un trabajador está compuesta por un salario base y unos complementos salariales. Con el teletrabajo desaparecen algunos complementos como los de puntualidad o asistencia, pero surgen otros de rendimiento y productividad, así como complementos de puesta a disposición, lo que se conoce como teledisponibilidad, que supone al trabajador estar a disposición de la empresa fuera del horario de trabajo y localizable para poder acudir a su puesto de trabajo en el momento en que sea necesario.

Esta característica del contrato de trabajo plantea problemas, sobre todo a la hora de la retribución, ya que el Estatuto de los Trabajadores sólo obliga a retribuir el tiempo de trabajo y los periodos de descanso asimilados al mismo, lo que significa que a la empresa no se le podrá exigir nada.

Pero es que además del aspecto retributivo, la teledisponibilidad plantea problemas al suponer una carga obligacional para el trabajador, no sólo física, ya que coarta su libertad de movimiento, sino también psicológica, al infundir en el teletrabajador la preocupación de tener que estar localizable y disponible en cualquier momento.

De ahí que la teledisponibilidad deba ser remunerada con independencia de la eventual prestación de servicios y deban pactarse sus condiciones en el contrato de teletrabajo o regularse en los convenios colectivos aplicables, para que no llegue a suponer un abuso en perjuicio del trabajador.

El tercer elemento de un contrato de trabajo es el ***temporal,*** de manera que los contratos de trabajo pueden tener una duración definida y temporalmente limitada, o bien indefinida en el tiempo, a tiempo completo o a tiempo parcial.

Una de las características del teletrabajador en relación con el tiempo dedicado al trabajo es que, al no desplazarse al centro de trabajo para desarrollar su actividad, puede repartir el tiempo que dedique al trabajo como tenga por conveniente o como mejor se adecue a sus circunstancias personales.

Esta circunstancia, es cierto que favorece al trabajador en el sentido de darle mayor libertad de organización y administración de su tiempo de trabajo, pero no es menos cierto que la no sujeción a un horario fijo puede llegar a suponer una invasión del trabajo en espacios reservados al descanso, la familia o el ocio, lo que implica la necesidad de procurar una efectiva ordenación del tiempo de trabajo y de los tiempos de descanso.

Otro aspecto a considerar es el de la jornada laboral, ya que en el derecho laboral esta figura delimita muchos aspectos de su régimen jurídico, como el tiempo máximo de trabajo a la semana, el salario que corresponde al trabajador atendiendo, entre otros aspectos, a la jornada de trabajo que realice, sea ésta entera o reducida, los descansos mínimos que en proporción al tiempo de trabajo le correspondan y tiempos de exposición a la pantalla con el fin de proteger la salud del teletrabajador.

En relación con el tiempo dedicado al trabajo podemos considerar estos otros aspectos:

- El teletrabajador pasa de tener una jornada laboral definida a compaginar el cumplimiento y establecimiento de límites máximos de jornada con la flexibilidad por parte del trabajador de organizársela libremente.
- La distribución del teletrabajo puede variar desde que el empresario fije unas bandas de trabajo en las que se desarrolle el mismo, hasta que sea el teletrabajador el que libremente se organice los tiempos de trabajo atendiendo a la demanda.

Un cuarto elemento es el ***formal,*** pudiendo el contrato de trabajo celebrarse de forma escrita o verbal, presumiéndose, en todo caso, existente *entre todo el que presta un servicio por cuenta y dentro del ámbito de organización y dirección de otro y el que lo recibe a cambio de una retribución a aquél,* según lo dispuesto en el art. 8.1 del Estatuto de los Trabajadores.

Tampoco se exige por tanto forma alguna para el contrato de teletrabajo, si bien es importante tener presente la cantidad de especialidades que reviste y considerar las ventajas de celebrar este contrato por escrito de forma que queden así fijados todos y cada uno de los matices del mismo.

De este modo queremos señalar algunas de las cláusulas contractuales especiales, siendo las más relevantes:

- ***Propiedad intelectual:*** cláusula por la que se pactará que la propiedad de todas las obras intelectuales desarrolladas por el teletrabajador es de la empresa.
- ***Exclusividad:*** la finalidad principal de esta cláusula es la de asegurar al empresario los servicios del trabajador de manera única. Esta exclusividad debe ir acompañada de una retribución económica para el trabajador.

- ***Confidencialidad y secreto:*** con esta cláusula se pretende que la información a la que el trabajador tenga acceso como consecuencia de su actividad laboral, dado que es propiedad de la empresa y para ésta tiene un gran valor, sea confidencial y quede garantizado que el trabajador guardará secreto sobre la misma.
- ***No competencia contractual y post-contractual:*** con el fin de que el empresario se asegure de que el teletrabajador no irá a la competencia ni durante ni tiempo después de extinguido el contrato, asegurándose así que el trabajo encargado al trabajador por él no sirva para beneficio de otros competidores.
- ***Custodia y restitución del material:*** el teletrabajador estará obligado a guardar la documentación que maneje y a devolverla a la empresa.
- ***Posibilidad de control por parte del empresario del uso de herramientas de trabajo puestas a disposición del trabajador***: de igual manera que si trabajara en la empresa, pero atendiendo a las circunstancias específicas.
- ***Tratamiento y protección de datos:*** deberá hacerse constar que el empresario es quien debe adoptar las medidas necesarias para garantizar la protección de los datos a los que vaya a acceder o vaya a tratar el teletrabajador para el desarrollo de sus funciones, quien, a su vez, deberá cumplir las normas que la empresa le imponga a tal fin.
- ***Condiciones laborales:*** serán las específicas de cada modalidad contractual.

Finalmente, en cuanto al **lugar** en que puede desarrollarse la actividad laboral, cabe que ésta se realice en el centro de trabajo de la empresa, o bien en otro lugar distinto. De esta forma el teletrabajo rompe con la definición de centro de trabajo y la sustituye por la de lugar de trabajo, ya que los teletrabajadores pueden prestar sus servicios desde diferentes ubicaciones, lo que plantea el problema de determinar su adscripción a un verdadero centro de trabajo, necesaria tanto para poder dar de alta al teletrabajador en la Seguridad Social como para determinar la representación laboral en función del número de trabajadores pertenecientes a un mismo centro.

Un aspecto importante a tener en cuenta en relación con el lugar en el que se desarrolla la prestación laboral es la referente a la obligación del empresario de garantizar las adecuadas condiciones de salud e higiene en el trabajo. Cuando el trabajo se desarrolla en el domicilio, siendo éste inviolable, el empresario ya no está legitimado para entrar y comprobar si se están utilizando debidamente las medidas de protección puestas a disposición del trabajador si no media su consentimiento expreso, que también será necesario para que pueda llevarse a cabo una inspección de trabajo. En relación con la seguridad e higiene en el teletrabajo, nos remitimos al apartado en el que tratamos esta cuestión.

b. Contenido del contrato

- **Condiciones:**
  - Horas de trabajo: Conviene pactar un número de horas diarias o semanales, además de establecer un sistema que permita justificar las horas de trabajo, aunque debe tenerse en cuenta que en el teletrabajo importa, sobre todo, el resultado, no tanto el tiempo empleado en conseguirlo.
  - Lugar de trabajo: En su caso, determinar las condiciones mínimas que debe reunir el lugar en que vaya a prestarse el trabajo.
  - Accesibilidad del trabajador: Establecer los momentos del día y los días a la semana que el teletrabajador debe estar disponible para la empresa.
  - Vacaciones.

- **Métodos de trabajo:** Determinar los medios a través de los cuales debe comunicarse el teletrabajador con la empresa (teléfono, fax, correo electrónico, ...), cada cuánto tiempo, a quién debe dirigirse, etc.
- **Remuneración:** En su caso, fijar el salario base y los complementos salariales a que tendrá derecho el teletrabajador.
- **Formación:** Conviene concretar si el teletrabajador va a recibir formación y, en su caso, de qué tipo, cuándo se va a impartir (al inicio del teletrabajo, formación continua...), si se va a insertar en los planes de formación de la empresa, etc.
- **Terminación de la situación de teletrabajo:** Lo habitual es que cualquiera de las partes (empresario o trabajador) pueda decidir en cualquier momento terminar la situación de teletrabajo, si bien suele establecerse un periodo de preaviso mínimo de entre tres y cinco meses.

En cualquier caso, la terminación del teletrabajo no tiene que afectar necesariamente a la vigencia del contrato de trabajo.

- **Propiedad y mantenimiento del equipo de trabajo:** Generalmente, el equipo de trabajo pertenece a la empresa, en cuyo caso será ésta quien se lo proporcione al trabajador, lo instale y se ocupe de su mantenimiento, debiendo determinarse en el contrato cada cuánto tiempo se va a realizar, si será el servicio técnico de la propia empresa o se externalizará, etc.

Asimismo, conviene determinar quién está autorizado a utilizar el equipo informático y si sólo con fines profesionales o también para uso personal.

- **Gastos:** Es importante determinar los costes que van a ser soportados por el empresario y aquéllos de los que deberá hacerse cargo el teletrabajador, así como los gastos que, aun siendo asumidos por el trabajador, le serán reembolsados o compensados por la empresa, cuándo y de qué forma.

La existencia de diversas modalidades de teletrabajo implica la existencia de gastos propios de cada una de dichas modalidades, como puedan ser las dietas y desplazamientos en el teletrabajo móvil o el pago del uso o alquiler del centro en el teletrabajo en telecentro, cuya responsabilidad deberá quedar también determinada.

- **Seguros:** Conviene determinar qué aspectos van a estar cubiertos por pólizas de seguros, a quien corresponde contratarlas y quién debe hacerse cargo de su coste.
- **Confidencialidad y seguridad de los datos:** A la empresa le interesará proteger la confidencialidad de su información, para lo cual podrá establecer claves de acceso a la información, adoptar sistemas de seguridad en el domicilio, etc.

5.5. Problemas que derivan del teletrabajo

Entre los problemas que derivan directamente del teletrabajo encontramos el hecho de que Internet es una red universal que permite a una persona trabajar desde un país para un empresario residente en otro país. El problema empieza cuando surgen conflictos entre el teletrabajador y el empresario y no se sabe qué legislación aplicar.

En defecto de una regulación específica, debe acudirse al Convenio de Roma, en virtud del cual se dará libertad a las partes para designar el derecho aplicable a su relación, siempre y cuando el trabajador no resulte desprotegido.

En defecto de acuerdo, y si el contrato no hace referencia a cual debe ser la legislación aplicable, entonces será la del país en que el trabajador realice su prestación, y si se realiza en varios, entonces la del lugar del establecimiento que le hubiere contratado.

Ahora bien, las modalidades de trabajo *on line* y *one way line* plantean la dificultad añadida de determinar qué se considera lugar de trabajo, si aquél en que se encuentra ubicado el trabajador o donde se halla la empresa, que es donde en realidad se está desarrollando el trabajo.

El teletrabajo también puede dar pie a abusos de mano de obra barata porque, al fin y al cabo, la conexión entre el trabajo y el empresario se realiza *on line* y para ello, lo mismo da que proceda del mismo país o de otro.

Por otra parte, y en la medida en que el teletrabajo utiliza Internet como soporte, de su puesta en práctica pueden derivar problemas que afecten a la seguridad informática, tales como virus, estafas y delincuencia, espionaje industrial, mal uso de los datos reservados o personales, etc.

Asimismo, al igual que cualquier otro trabajador, los teletrabajadores tienen derecho a que la empresa invierta en su formación, si bien se complica sobremanera el que el empresario pueda completar esa formación a nivel práctico a distancia.

5.6. Particularidades de algunas facultades del empresario

a. Poder disciplinario

En el ámbito del teletrabajo, la posibilidad del empresario de ejercer su poder disciplinario para imponer sanciones se complica, bien como consecuencia de la inevitable falta de control, bien porque en la obtención de pruebas que permitan inculpar al teletrabajador pueda llegar a vulnerarse alguno de sus derechos fundamentales, lo que no deja de plantear dificultades y obliga a establecer mecanismos de control en función de la modalidad de teletrabajo que se haya establecido: a domicilio *on line,* a domicilio *off line* o en telecentro.

Ahora bien, todas las modalidades de teletrabajo conllevan, de un lado, o una limitación de la capacidad de control del empresario o, en ocasiones, un control demasiado exhaustivo cuyo principal riesgo es la posible vulneración de los derechos fundamentales del trabajador y, de otro lado, una modificación de lo que tradicionalmente han venido considerándose faltas del trabajador, en el caso del teletrabajo, perdiendo importancia unas (puntualidad o asistencia al trabajo) y ganándola otras ya existentes o apareciendo nuevas.

A través de la negociación colectiva deberá llegarse a una nueva tipificación de las faltas, siendo aconsejable una regulación lo más abierta posible, de manera que pueda contemplar cualquier conducta del trabajador que pudiera perjudicar a la empresa.

El nuevo código disciplinario habrá de incorporarse a los contratos de trabajo y deberá comunicarse a los teletrabajadores, siendo aconsejable una comunicación virtual, que ofrece mayores garantías en cuanto a su recepción al tratarse de trabajadores que con bastante frecuencia utilizan herramientas informáticas.

Sin embargo, la comunicación al teletrabajador de la comisión de una falta y de la imposición de su correspondiente sanción requiere una mayor certeza de en qué momento se produce la recepción, ya que está en juego la caducidad para impugnar la sanción impuesta.

b. Poder de dirección

Según se establece en el artículo 20.3 del ET, el empresario puede adoptar cuantas medidas de vigilancia y control estime oportunas para vigilar que el trabajador cumple con sus deberes y obligaciones laborales.

No obstante, este control se ve limitado, de un lado, por el hecho de que dichas medidas deben estar dirigidas única y exclusivamente a comprobar que efectivamente el trabajador está incumpliendo y, de otro lado, que sean medidas que no vulneren el derecho a la intimidad del trabajador.

La introducción de las Nuevas Tecnologías permite controlar incluso al teletrabajador, a pesar de no encontrarse físicamente en las oficinas de la empresa.

Este tipo de control se puede llevar a cabo, por ejemplo, a través de la instalación de videocámaras, si bien sólo en supuestos en los que se haga necesario para asegurar la protección de los bienes de la empresa.

Ante el teletrabajo en el domicilio, su utilización sólo será lícita si el trabajo se desempeña en una habitación en la que no se desarrolle la vida familiar y sólo si su conexión se realiza durante las horas en que se esté trabajando, previo conocimiento por el teletrabajador y una vez emitido un informe por los representantes de los trabajadores.

Otro tipo de control es el que se realiza sobre las llamadas, sin olvidar el derecho a la inviolabilidad de las comunicaciones, que sólo podrá verse limitado ante la necesidad de preservar otros derechos como el de vigilancia y dirección del empresario.

Lo que se pretende con este sistema es comprobar que el teléfono de la empresa es utilizado por el trabajador sólo con fines profesionales, especialmente cuando el trabajo se realice únicamente a través de la comunicación telefónica, a efectos de conocer cómo desarrolla el trabajador su trabajo, pero también para que los pedidos queden registrados ante posibles reclamaciones. En cualquier caso, siempre con el conocimiento del trabajador.

Sobre todo en el ámbito del teletrabajo, el control de Internet y del correo electrónico se hace necesario por ser, para una gran parte de los teletrabajadores, instrumentos o herramientas de trabajo, cuya inadecuada utilización puede ocasionar diversos perjuicios a la empresa.

Este tipo de control se justifica, entre otras razones, porque de los medios informáticos es propietaria la empresa, y por lo tanto no deben ser utilizados para uso personal, lo que no excluye que, en el ejercicio de este control debe procurarse no atentar a la intimidad o al secreto de las comunicaciones de los teletrabajadores.

La adopción de esta medida de control debe ser proporcionada, justificándose por la existencia de un interés legítimo por parte del empresario, que tenga sospechas razonables de la comisión de irregularidades en el puesto de trabajo.

Antes de llevar a cabo un registro, única y exclusivamente para fines profesionales, deberá informarse al trabajador y solicitar un informe a los representantes de los trabajadores.

c. Seguridad e Higiene

Si bien la responsabilidad de garantizar la salud en el trabajo es del empresario, cuando el trabajo se desarrolla en el domicilio, siendo éste inviolable, el empresario ya no está legitimado para entrar y comprobar si se están utilizando debidamente las medidas de protección puestas a disposición del trabajador si no media su consentimiento expreso, que también será necesario para que pueda llevarse a cabo una Inspección de Trabajo.

Luego, a pesar de que los teletrabajadores tengan los mismos derechos que los restantes trabajadores, según se desprende del Convenio 177 OIT, la responsabilidad del empresario debe limitarse a la puesta a disposición de los medios de protección necesarios, y a un control indirecto del uso de los mismos, y de darles una formación adecuada.

Si el teletrabajo es desarrollado en un telecentro, no habrá problemas de acceso para comprobar que se cumplen las medidas de seguridad exigidas, de cuya adopción será responsable el titular del telecentro.

Por su parte, el Real Decreto 488/1997, de 14 de abril, aplicable a los trabajadores que habitualmente y durante gran parte de su trabajo utilicen equipos informáticos, impone al empresario la obligación de

adoptar las medidas necesarias para evitar o reducir los riesgos derivados de la utilización de equipos con pantallas de visualización, en particular los posibles riesgos para la vista y los problemas físicos y de carga mental, teniendo en cuenta las características propias del puesto de trabajo y las exigencias de la tarea, en concreto las relativas a los tiempos de utilización del equipo y atención requeridos por la tarea.

Las lesiones sufridas por el trabajador durante el tiempo y en el lugar de trabajo se presume que son accidentes de trabajo, salvo prueba en contrario, según lo dispuesto en el art. 115.3 Ley General de la Seguridad Social[60], de manera que el trabajador sólo tendrá que demostrar el lugar y la hora del accidente si tiene un horario predeterminado.

No obstante, para los teletrabajadores, dado que son ellos quienes libremente fijan su horario, se invierte la carga de la prueba, de manera que a ellos corresponde demostrar la relación de causalidad entre el accidente y su trabajo.

5.7. Ventajas e inconvenientes de esta forma de trabajo

La experiencia del teletrabajo en distintas empresas y países ofrece una serie de aspectos comunes que vienen a constituir ventajas e inconvenientes, tanto desde la óptica del trabajador como de la empresa.

Ventajas
Para el trabajador:
• Incremento de las posibilidades de acceso en condiciones de igualdad a un puesto de trabajo para colectivos especiales de trabajadores (discapacitados, amas de casa, ...).
• Mayor autonomía profesional.
• Flexibilidad en la distribución del tiempo y en la utilización de los espacios.
• Posibilidad de conciliar la vida personal o familiar con la vida profesional.
• Mayor calidad de vida.
• Reducción de los costes y tiempos de desplazamiento (si el teletrabajo se realiza en el domicilio).
Para la empresa:
• Incremento de la productividad como consecuencia del ahorro de tiempo no productivo, de transporte y por la reducción de las tasas de absentismo.
• Disminución de costes (en equipamiento de los centros de trabajo, alquiler de oficinas, ...).
• Mayor facilidad de contratación de personal cualificado con independencia de su residencia.
• Flexibilidad en la organización del trabajo.
• Menor contaminación ambiental.
• Potencia el uso y conocimiento de las Tecnologías de la Información.

[60] *Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.*

Inconvenientes
Para el trabajador:
• Pérdida de integración en la empresa.
• Posibilidad de aislamiento personal o social.
• Dificultad para encontrar un apoyo laboral y obtener respuesta en tiempo breve a consultas que se puedan formular.
• Dificultad para separar el trabajo de la vida personal o la familia.
• Sobreexplotación y pérdida de privacidad.
• Asunción de costes por parte del trabajador que antes no soportaba (equipamiento, acondicionamiento de un lugar en el domicilio, incremento en los gastos de teléfono, ...).
• En ausencia de regulación laboral, el trabajador puede encontrarse desprotegido ante problemas como accidentes laborales, contratos, planes de jubilación...
Para la empresa:
• Incremento de costes en adaptación de la nueva organización del trabajo debido a posibles deficiencias en el intercambio de información o retrasos en la toma de decisiones.
• Dificultad de mantener la confidencialidad de los procedimientos e información de la empresa.
• Menor control sobre los trabajadores.
• Imposibilidad de supervisión directa del desarrollo del trabajo.
• Dificultad para motivar a los trabajadores a distancia y hacerles partícipes de los objetivos de la empresa lo que puede llevar a que ésta pierda parte de su fuerza corporativa.
• Pérdida de la atmósfera de trabajo en equipo.

5.8. Uso del correo electrónico y uso de Internet en el trabajo. Sistemas de videovigilancia

a. Introducción

El uso que los trabajadores realizan de las herramientas de trabajo que ofrecen las Nuevas Tecnologías a las empresas, tales como Internet, correo electrónico, teléfono móvil, entre otros, presenta dos intereses encontrados, el del empresario que quiere limitar el que el uso que de estos medios realice el trabajador sean lo más limitados al desarrollo de sus prestaciones laborales, que las consecuencias negativas que puedan limitarse del uso de estos medios por el trabajador, véase entrada de virus o comisión de acciones delictivas, estén controladas en algún extremo. Por su parte, el interés del trabajador, puede radicar, en limitar la inspección del empresario en el uso de estas herramientas de forma que no invada su intimidad.

Los medios que los empresarios tienen a su disposición para controlar el trabajo que realizan sus empleados, no pueden ser usados de tal forma que perjudiquen derechos y libertades de éstos. Del mismo modo que tampoco pueden ser medios para que el trabajador se beneficie a costa de la empresa, más allá de aquellas prestaciones para las que la empresa haya decidido poner a disposición de los trabajadores los medios de los que se trate.

En la búsqueda del equilibrio de estos intereses contrapuestos el Dictamen 8/2001 del Grupo de Trabajo del "Artículo 29" [61] de la Directiva 95/46/CE relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo, adoptado el 13 de septiembre de 2001, recoge un conjunto de principios que deben regir las relaciones que examinamos, estos principios son:

1. Que la prevención debe prevalecer sobre la detección, ya que al plantearse la utilización de Internet o del correo electrónico con fines privados, considera que es mejor para el empresario prevenir la utilización abusiva de Internet que detectarla.
2. Información al trabajador de:

   (i) La presencia, utilización y objetivo de todo equipo y/o aparato de detección activado en su puesto de trabajo, así como

   (ii) Cualquier abuso de las comunicaciones electrónicas detectado (correo electrónico o Internet), salvo si existen razones imperiosas que justifiquen la continuación de la vigilancia encubierta, lo que normalmente no sucede. Puede transmitirse información rápida fácilmente mediante un programa informático, por ejemplo ventanas de advertencia que avisen al trabajador de que el sistema ha detectado y/o tomado medidas para evitar una utilización ilícita de la red.

b. Vigilancia

Si bien los trabajadores tienen derecho a un cierto grado de respeto de la vida privada en el trabajo, este derecho no debe lesionar el derecho del empresario de controlar el funcionamiento de su empresa y de protegerse contra una actuación de los trabajadores susceptible de perjudicar sus intereses legítimos, por ejemplo la responsabilidad del empresario por acciones de sus trabajadores.

c. Secreto de correspondencia

Actualmente cuando hablamos de correspondencia debemos entender incluidas además de los documentos en soporte papel, también otras formas de comunicación electrónica recibida o enviada en el lugar de trabajo, como las llamadas efectuadas o recibidas en locales profesionales o los mensajes electrónicos recibidos o enviados en ordenadores puestos a disposición del lugar de trabajo.

Desde el punto de vista del empresario, puede plantearse la cuestión que examinamos como que desde el momento en el que éste informa al trabajador de que utiliza medios de control de las comunicaciones que realiza desde su puesto de trabajo y utilizando medios de la empresa, no tenga derecho a adecuada protección de su derecho a la intimidad.

Al referirnos a los correos electrónicos como medio de correspondencia debemos entender incluidos en los mismos los ficheros que estos correos lleven adjuntos y en este sentido considerar que los correos electrónicos proceden de un remitente al que no se tiene oportunidad de informar del control de vigilancia que se va a realizar sobre las comunicaciones que realice a nuestro empleado.

d. Protección de datos

Sin perjuicio de lo que desarrollaremos extensamente al tratar la materia de protección de datos en sí misma, entendemos necesario realizar en este apartado una breve referencia a la misma destacando algunas consideraciones básicas.

Los principios de protección de datos deben respetarse en el tratamiento de los datos personales que implica este tipo de vigilancia. Para que una actividad de control sea legal y se justifique, deben respetarse todos los principios siguientes:

---

[61] *El Grupo de Trabajo del "Artículo 29" de la Directiva 95/46/CE es un grupo consultivo independiente, de asesoramiento a la Comisión Europea, compuesto por representantes de las autoridades de los Estados miembros encargadas de la protección de datos, cuya misión es, en particular, examinar todas las cuestiones relativas a la aplicación de las medidas nacionales adoptadas en virtud de la Directiva sobre protección de datos con el fin de contribuir a su aplicación uniforme.*

A. Principio de necesidad

Esto es cuando sea justificado por una finalidad que necesariamente implique la adopción de estas medidas.

De este modo, sólo en circunstancias excepcionales se considerará necesaria la vigilancia del correo electrónico o de la utilización de Internet de un trabajador. En el caso de resultar necesario controlar el correo electrónico de un trabajador para obtener una confirmación o una prueba de determinados actos del mismo. En este tipo de actos se incluiría la actividad delictiva de un trabajador que obligara al empresario a defender sus intereses, por ejemplo, cuando es responsable subsidiario de los actos del trabajador. Estas actividades de vigilancia incluirían también la detección de virus y, en general, cualquier actividad realizada por el empresario para garantizar la seguridad del sistema.

La apertura del correo electrónico de un trabajador puede también resultar necesaria por razones distintas del control o la vigilancia, por ejemplo para mantener la correspondencia cuando el trabajador está ausente o cuando la correspondencia no puede garantizarse de otra forma.

De este principio de necesidad se deduce que el empresario no puede, una vez transcurridas las circunstancias para la acción de vigilancia, seguir conservando estos datos del trabajador, atendiendo a las reglas de la protección de datos deberá proceder a cancelarlos.

B. Principio de transparencia

Este principio significa que un empresario debe indicar de forma clara y abierta sus actividades.

La obligación de proporcionar información al interesado:

Significa que el empresario debe transmitir a su personal una declaración clara, precisa y fácilmente accesible de su política relativa a la vigilancia del correo electrónico y la utilización de Internet.

Los trabajadores deben ser informados de manera completa sobre las circunstancias particulares que pueden justificar esta medida excepcional; así como del alcance y el ámbito de aplicación de este control. Esta información debería incluir:

1. *La política de la empresa* en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización).
2. *Los motivos y finalidad de la vigilancia,* en su caso. Cuando el empresario autorice a los trabajadores a utilizar los sistemas de comunicación de la empresa con fines personales, las comunicaciones privadas podrán supervisarse en circunstancias muy limitadas, p. ej. para garantizar la seguridad del sistema informático (detección de virus).
3. *Información detallada sobre las medidas de vigilancia adoptadas,* p. ej. ¿quién?, ¿qué?, ¿cómo? y ¿cuándo?
4. *Información detallada sobre los procedimientos de aplicación,* precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos.

Es posible que los convenios colectivos no sólo obliguen al empresario a informar y consultar a los representantes de los trabajadores antes de instalar sistemas de vigilancia, sino que también supediten esta instalación a su consentimiento previo. Asimismo, en los convenios colectivos pueden establecerse los límites de la utilización de Internet y del correo electrónico por los trabajadores, así como proporcionarse información detallada sobre el control de esta utilización.

C. Principio de legitimidad

Este principio significa que una operación de tratamiento de datos sólo puede efectuarse si su finalidad es legítima, esto es, el tratamiento de los datos de un trabajador debe ser necesario para la satisfacción del interés legítimo perseguido por el empresario y no perjudicar los derechos fundamentales de los trabajadores.

La necesidad del empresario de proteger su empresa de amenazas importantes, por ejemplo para evitar la transmisión de información confidencial a un competidor, puede considerarse un interés legítimo.

D. Principio de proporcionalidad

Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empresario.

Cuando el acceso al contenido de los mensajes sea indispensable, convendría tener en cuenta el respeto de la vida privada de los destinatarios externos e internos de la organización. El empresario no puede obtener el consentimiento de las personas ajenas a la organización que envían mensajes a los miembros de su personal así como tampoco debería aplicar todos los medios razonables para informar a las personas ajenas a la organización de la existencia de actividades de vigilancia que pudieran afectarlas. Una forma de cumplir esto sería la de insertar avisos de la existencia de sistemas de vigilancia en todos los mensajes salientes de la organización.

Del mismo modo que la tecnología ofrece al empresario importantes posibilidades de evaluar la utilización del correo electrónico por sus trabajadores, puede también utilizarse para garantizar que sean proporcionadas las medidas adoptadas por el empresario para proteger de todo abuso el acceso a Internet autorizado a su personal, utilizando mecanismos de bloqueo más que de vigilancia.

E. Principio de exactitud y conservación de los datos

Este principio requiere que todos los datos legítimamente almacenados por un empresario que incluyan datos procedentes de una cuenta de correo electrónico de un trabajador, de su utilización de Internet o relativos a las mismas deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. Los empresarios deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales.

F. Principio de seguridad

Desde el punto de vista de la protección de datos este principio obliga al empresario a aplicar las medidas técnicas y organizativas adecuadas para proteger todos los datos personales en su poder de toda intromisión exterior.

Incluye también el derecho del empresario a proteger su sistema contra los virus y puede implicar el análisis automatizado de los mensajes electrónicos y de los datos relativos al tráfico en la red.

El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, siempre y cuando existan garantías adecuadas y considera que es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder.

capítulo quinto

Fiscalidad en el comercio electrónico

1. INTRODUCCIÓN

Con la entrada en vigor de la LCE, aumenta el número de oportunidades para el comercio electrónico internacional y consecuentemente, aumenta la competitividad entre las empresas de los diferentes Estados.

El desarrollo del comercio electrónico, ha incidido de manera significativa en el impulso y progreso de las iniciativas empresariales. Sin embargo, los sistemas tributarios actuales no están adaptados a los cambios que requiere la globalización.

Los sistemas tributarios tienen y han tenido tradicionalmente un carácter nacionalista. Con la llegada de la globalización se pone en cuestión la eficiencia de los sistemas jurídicos basados en la soberanía nacional y por eso las organizaciones internacionales juegan un papel muy relevante en la solución fiscal a los problemas de la internacionalización.

A medida que las restricciones normativas desaparecen, los obstáculos fiscales persistentes cada vez son más patentes, y la fiscalidad resulta uno de los ámbitos más relevantes en los que el Mercado Único no llega a implantarse.

2. INCIDENCIA EN EL COMERCIO ELECTRÓNICO

El comercio electrónico representa un reto para la fiscalidad y, con las Nuevas Tecnologías, las transacciones imponibles se aíslan del ámbito de aplicación territorial común de impuestos basados en la territorialidad; y, al mismo tiempo, las discordancias normativas nacionales favorecen cada vez más la evasión fiscal.

En este sentido, la Unión Europea aboga por el diseño de un marco legal para la fiscalización y tributación del comercio electrónico partiendo del ordenamiento y de los procedimientos tributarios vigentes, de manera que estos modelos fiscales en funcionamiento se adapten a las necesidades del comercio electrónico, frente a otros países, como Estados Unidos, que promueven la implantación de sistemas tributarios específicos y únicos para Internet, habiendo llegado incluso a proclamar la no imposición por un tiempo. Un ejemplo de este sistema especial lo constituye el polémico y descartado planteamiento conocido como bit tax que contempla gravar sobre el número de bits transmitidos.

Este sistema de bit tax es criticado por sus detractores que lo acusan de injusto, porque no grava en relación proporcional al valor de las transacciones y de ineficaz, porque no puede distinguir las transacciones comerciales de las que no lo son y por su obsolescencia técnica.

Esta alternativa a la tributación tradicional en el comercio electrónico consistente en gravar cada impulso electrónico transmitido en las comunicaciones electrónicas, en la Red en especial, presenta además como inconveniente que se necesitaría la constitución de una autoridad internacional de control tributario. También existen razones éticas que lo rechazan (porque es un sistema injusto en el que no se gravarían las transacciones proporcionalmente a su valor) y dificultades técnicas (porque resulta casi imposible discernir cuándo se está ante una transacción económica en una comunicación y porque es un sistema tecnológicamente obsoleto).

En este sentido, el Consejo Europeo [COM (2000) 349 final] entiende que no es necesario crear ningún impuesto nuevo o adicional, sino adaptar los existentes y, en particular, el Impuesto sobre Valor Añadido, en adelante I.V.A., al consumo; que las entregas de productos en forma electrónica deben considerarse prestaciones de servicios, y que el I.V.A. tiene que aplicarse en el territorio en el que se produce el consumo, es decir, sólo las prestaciones de servicios consumidas en Europa deben gravarse en Europa.

Por su parte, la autorregulación, perseguida por ordenamientos anglosajones muy proclives a la misma, y en especial por Estados Unidos, podría llevar a impuestos muy bajos o inexistentes y a las pérdidas consecuentes en los países receptores de los servicios. Los países partidarios de la regulación legal, entre los que figura España, afirman que la autorregulación lesionaría los principios tributarios de equidad, neutralidad y eficiencia.

3. PROBLEMAS DE FISCALIDAD EN INTERNET

Se han identificado distintas áreas que generan problemas en relación con la fiscalización de Internet. Así, se señalan como dificultades para la Administración Tributaria la identificación del contribuyente, la información tributaria y la recaudación y control tributarios.

Por un lado, en relación con los impuestos al consumo hay que delimitar el lugar de consumo, la clasificación de los productos digitales y la recaudación de dichos impuestos en concreto.

Por otro lado, se plantean problemas de carácter general como la ubicación de las compañías en "paraísos informáticos" o los conflictos entre las distintas jurisdicciones, que dificultan el desarrollo de la tributación del comercio electrónico.

Se hace así imprescindible la cooperación internacional para diseñar Acuerdos Internacionales sobre imposición que eliminen las deficiencias creadas por, entre otros aspectos, los precios de transferencia y la doble imposición.

Los precios de transferencia son de nuevo uno de los problemas ya tradicionales en el Derecho Tributario pero que se agrava como consecuencia de la internacionalización. Además de por la proliferación en su utilización, la situación empeora fruto de los bienes transferidos. Por ejemplo, los productos de software, o la adquisición de derechos de propiedad industrial, o la traslación del Know How obtenido consecuencia de una fuerte previa inversión en I+D. Todas estos representan transacciones difícilmente cuantificables y por lo tanto difícilmente controlables.

El Principio de igualdad de trato *(arm´s length)* está muy relacionado con la problemática de los precios de transferencia, pues cuando se realizan transacciones entre dos partes dependientes entre sí o de un tercero, los precios fijados pueden diferir de los que hubieran sido fijados de haberse realizado entre partes independientes. No obstante, es un principio de difícil aplicación práctica, pues los precios de mercado no están normalmente disponibles por diversas razones, bien porque no sean transacciones equiparables o porque se trate de transacciones de productos intermedios sin entidad por sí mismos o, más concretamente, en el caso de bienes intangibles, como el software o los derechos de propiedad industrial, como las patentes o las marcas. Algunas legislaciones nacionales permiten a las Administraciones Tributarias ajustar los precios de transferencia a efectos tributarios en aplicación del principio de igualdad de trato.

La fiscalización en el comercio electrónico conlleva problemas tanto en el ámbito de la imposición directa como en la imposición indirecta. En definitiva, la generalización del comercio electrónico va a afectar como consecuencia de las dificultades existentes a la hora de identificar a los intervinientes, de calificar las rentas o de localización geográfica, a aquellos impuestos que, en general, graven las rentas de las personas físicas o jurídicas (tributación directa). Asimismo, existen problemas con los impuestos relativos al consumo y, en general, con la tributación indirecta.

4. IMPOSICIÓN DIRECTA

En relación con la imposición directa, el Impuesto sobre la Renta de las Personas Físicas no va a verse especialmente afectado por el desarrollo del comercio electrónico. El problema fundamental será el de la localización de las rentas, es decir, determinar la situación de una persona en un territorio con el objeto de establecer el lugar de residencia del sujeto pasivo que tributará por este concepto. El Impuesto sobre Sociedades y el Impuesto sobre la Renta de los no Residentes generan problemas relativos a la calificación de las rentas, la localización de los sujetos y al concepto de establecimiento permanente (EP). Analicemos brevemente estos problemas:

a. *La calificación de las rentas* obtenidas cuando se produce una compraventa electrónica plantea dos supuestos diferenciados. De un lado, en el comercio electrónico directo, esto es, la transmisión de bienes y/o servicios digitalizados puede consistir sólo en un derecho de uso o una compraventa de estos productos que sólo difiere de la compraventa de bienes físicos en el soporte utilizado.

En términos tributarios, la cesión de uso puede entenderse que genera un canon cuya renta se considera obtenida en España, según lo dispuesto en el artículo 12.1 de la Ley de Renta de no Residentes[62], o puede entenderse como una compraventa internacional que se somete a tributación en el Estado de residencia del proveedor en virtud del artículo 12.3 de la misma ley.

La tributación del software está causando muchas dudas precisamente en la diferenciación entre cesión de uso y compraventa.

Las rentas se pueden calificar en beneficio empresarial, canon y otras rentas. Como reglas generales: los beneficios empresariales se gravan en el Estado de residencia que los obtiene, por lo que aquí el concepto de EP es vital, pues la parte de renta imputable a este EP será gravada en el país de localización del mismo; los cánones se gravan en el país de residencia del beneficiario y afectan a gran cantidad de bienes como los que se encuadran en la propiedad industrial o intelectual; las otras rentas, con carácter general tributan en el país de residencia del transmitente del bien.

b. Los problemas de *localización de los sujetos intervinientes* crean graves conflictos en la tributación directa. Pues si bien existe un consenso generalizado sobre la primacía del criterio personal o subjetivo frente al objetivo a efectos de tributación, los Estados también utilizan el criterio territorial de aplicación del impuesto. En definitiva, en principio prevalece el Estado de residencia sobre el Estado de la fuente. Pero en contratación electrónica, la dificultad para localizar a los sujetos intervinientes es muy importante, tanto el proveedor de servicios, que incluso puede manipular su dirección física en la página web para acogerse a normativas favorables a efectos fiscales, como el adquirente, teniendo en cuenta la facilidad para el anonimato que proporciona Internet.

Actualmente, y aunque tradicionalmente los Convenios para evitar la Doble Imposición han impuesto las ventajas de la tributación en el Estado de residencia, las tendencias reclaman la vía del criterio de territorialidad y en consecuencia del Estado de consumo-fuente para la tributación, tanto directa como indirecta, del comercio electrónico.

c. El concepto de *establecimiento permanente* (EP) alude a un organismo autónomo desde el punto de vista impositivo pero dependiente jurídicamente hablando de una entidad matriz establecida en otro

[62] *Ley 41/1998, de 9 de diciembre, sobre la Renta de no Residentes y Normas Tributarias (B.O.E. núm. 295, de 10 de diciembre).*

Estado. Así, el Estado del establecimiento permanente se denomina Estado de la fuente y el de la entidad matriz Estado de residencia.

La Ley de renta de no Residentes requiere que exista un lugar fijo de negocios para permitir el gravamen de las rentas generadas en este lugar fijo. Evidentemente, este concepto puede llegar a constituir un concepto jurídico indeterminado cuya interpretación amplíe o disminuya la obligación de tributar, por lo que, una vez que se determina la existencia de este lugar fijo de negocios, se necesita asimismo que la actividad desarrollada tenga cierta importancia, y por ende, cierta independencia logística y en términos de beneficios, de la casa matriz.

Este concepto ya parte del Modelo de Convenio de la OCDE según el cual el EP es *un lugar fijo de negocios mediante el cual una empresa desarrolla toda o parte de su actividad.* Evidentemente, el contexto electrónico aumenta sobremanera los problemas de determinación efectiva del EP, y que si atendemos a la definición del Modelo de Convenio de la OCDE la falta de presencia física elimine la posibilidad de reconocer un EP en un país.

Además, el modelo de tributación de los EP, por diferencia entre ingresos y gastos, dificulta también la adjudicación de los mismos a un EP concreto que los genera por sus operaciones electrónicas que a la vez incluyen a diversos agentes en su desarrollo a los que serán imputables proporcionalmente los gastos e ingresos generales.

5. IMPOSICIÓN INDIRECTA

Impuesto sobre el Valor Añadido (I.V.A.)

La imposición indirecta constituye una de las fuentes más antiguas de ingresos gubernamentales. Son impuestos que recaen sobre determinadas transacciones, bienes o servicios, y que en igual medida se ve afectada por las transacciones comerciales electrónicas. No sólo existen los problemas respecto al I.V.A. o a los impuestos al consumo en general. También hay dificultades de control respecto a otros tributos indirectos como puede ser el caso del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados en el caso de la legislación española, tanto nacional como local.

El I.V.A. grava dos hechos imponibles, las entregas de bienes y las prestaciones de servicios, pudiendo ser ambos consecuencia del comercio electrónico, incluyendo dentro de las prestaciones de servicios las entregas de productos en forma electrónica. Tratar una transacción de una manera u otra tiene sus consecuencias impositivas, pues en el caso de las entregas de bienes se localizan en el lugar donde el cliente dispone efectivamente del bien, y las prestaciones de servicios hay que localizarlas en el país de sede efectiva del prestador de servicios, aunque con excepciones, como las que prescribe la Ley española del I.V.A. [63], que asume localizados en el territorio español cuando el destinatario sea un empresario o profesional y su sede de actividad la tenga en España, o tenga un EP, o su lugar de domicilio, las cesiones de derechos de propiedad industrial e intelectual, los servicios de publicidad, el tratamiento de datos por procedimientos informáticos, el suministro de informaciones y los servicios de telecomunicaciones en los casos previstos en la citada Ley.

En cuanto la provisión en línea de productos digitales se trata de un nuevo tipo de transacción comercial cuya catalogación se encuentra en discusión internacional. A efectos del I.V.A. la UE la considera una prestación de servicios.

La localización de los activos a efectos fiscales resulta de extraordinaria importancia respecto del I.V.A. en el que la localización de los bienes en cuestión puede determinar su aplicabilidad, esto es, el I.V.A. sólo se paga si el suministro de los productos se realiza en un país sujeto a I.V.A.

En este sentido, los Impuestos Especiales (II.EE.) no están armonizados dentro de la Unión Europea y la globalización del comercio acentúa el problema, que tradicionalmente se ha venido dando en el

[63] *Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.*

comercio internacional, puesto que si los Estados incrementan ciertos impuestos se puede generar una pérdida de actividad económica y a su vez un aumento en los ingresos del país vecino con los tipos impositivos menores.

Las mercancías materiales compradas por consumidores privados por vía electrónica pero suministradas por vía tradicional, a efectos de I.V.A. se tratan de la misma forma que cualquier otra forma de venta a distancia, es decir, las mercancías compradas en países terceros se gravan a la importación, las exportadas son a tipo cero y las ventas intracomunitarias se gravan en el país del vendedor o del comprador dependiendo en gran medida del volumen de transacciones realizadas por el vendedor.

El I.V.A. se ve amenazado por el creciente número de servicios internacionales que gracias a las Nuevas Tecnologías sitúan las transacciones imponibles fuera del ámbito territorial de aplicación del sistema común del I.V.A., a la vez que las divergencias entre las normativas nacionales favorecen cada vez más la evasión fiscal.

El régimen de impuestos indirectos en la UE y los de sus socios comerciales debería ser neutral y el carácter global y general de impuesto sobre el consumo del I.V.A. europeo hace que existan diferencias entre los suministros intracomunitarios y los suministros a países terceros. Incluso, dentro de la UE habría que atender a las diferencias entre sus miembros. En este sentido, si se opta por aplicar el I.V.A. del país de origen a los productos digitales vendidos electrónicamente algunos países europeos perderían competitividad actualmente frente al resto como es el caso de Irlanda que tiene un gravamen del 21% lo que la sitúa con Bélgica en una hipotética tercera posición en la clasificación del I.V.A..

Además, el Consejo de la Unión Europea también se preocupa por el control y la aplicación del I.V.A. sobre el comercio electrónico, sobre la necesidad de la normativa sobre facturación electrónica, sobre facilitar el cumplimiento de las normas por los usuarios del comercio electrónico y sobre la necesidad de prever el cumplimiento por vía electrónica de las obligaciones fiscales.

Dado el crecimiento del comercio de bienes y servicios intangibles hay que corregir las deficiencias legales que no permiten garantizar que estos servicios puedan ser exportados exentos de derechos ni que se pueda aplicar el I.V.A. a los consumidores privados de la UE por operadores extranjeros.

Estas circunstancias, además de falsear la competencia, colocan en una posición de desventaja comparativa a los proveedores europeos. Las modificaciones propuestas por el Consejo apuestan por mantener en la medida de lo posible el sistema actual. De este modo, los prestadores de servicios tienen que poder distinguir entre clientes comerciales (sujetos pasivos) y consumidores finales (personas no imponibles). Esto que en el medio tradicional constituye la manera normal de actuar requerirá de la implantación de los medios tecnológicos necesarios para su funcionamiento, por ejemplo, a efectos de comprobación en línea del número de identificación del sujeto pasivo del I.V.A.. Las prestaciones a personas no imponibles quedan iguales, es decir, se aplica el I.V.A. en el Estado miembro del vendedor y para clientes fuera de la UE se propone una exclusión del I.V.A. en las prestaciones electrónicas.

Los prestadores de servicios establecidos en terceros países tendrán que aplicar y declarar el I.V.A. en las ventas a consumidores finales establecidos en la UE, pero se simplificará la normativa al máximo.

Las empresas deben tener en cuenta distintos aspectos para tomar una decisión correcta en cuanto a la fiscalidad aplicable: la situación fiscal del cliente, es decir, si el comprador está registrado a efectos de I.V.A. o si es un consumidor privado; si se trata de un consumidor privado o establecido fuera de la UE (con los ya mencionados problemas de identificación de las partes intervinientes en el comercio electrónico) se deberá determinar la jurisdicción competente, siendo el objetivo verificar el lugar de consumo, y el tipo de impuesto aplicable a la transacción siendo en las ventas a consumidores en la UE el I.V.A. del Estado miembro en el que esté registrado el prestador de servicios.

Sin embargo, con la irrupción de las Nuevas Tecnologías, no se pone en cuestión los conceptos subyacentes al criterio de la localización, sino, sobre todo, la dificultad añadida de, en primera instancia, su determinación y, subsidiariamente, su control. Por tanto, a pesar de que la doctrina ha calificado

estas normas de localización como “normas formales”, en contraposición a las “normas sustanciales” que determinan de forma concreta el tratamiento tributario de los objetos imponibles, lo cierto es que es imprescindible su determinación primaria para cualquier imposición tributaria específica posterior.

En definitiva, en toda transacción a efectos de I.V.A. tendrá que determinar su calificación como entrega de bien o como prestación de servicios y la categoría de esta última en su caso, así como la localización del hecho imponible.

Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados (ITPAJD)

El ámbito objetivo de aplicación de este impuesto recae sobre las transmisiones onerosas de bienes y derechos que estén situados o puedan ejercitarse o deban cumplirse en España. Esta regla, aplicable en su totalidad en caso de bienes inmuebles, se completa con el criterio de residencia que se aplica a los demás bienes y derechos propiedad de un sujeto pasivo residente en España cuando el contrato se haya celebrado en territorio español sobre bienes situados en el extranjero.

Impuestos Especiales (II.EE.)

Los impuestos especiales no están absolutamente armonizados dentro de la UE. Las disparidades, principalmente entre las tres categorías principales de productos sujetos a estos impuestos, como el tabaco, los hidrocarburos y las bebidas alcohólicas, conllevan problemas en política fiscal nacional. Si los Estados incrementan dichos impuestos se puede generar una pérdida de actividad económica y la consecuente generación de ingresos en un país vecino con tipos impositivos menores. Si esto ya ocurría en el comercio internacional tradicional, es evidente que la globalización del comercio gracias al uso de las Nuevas Tecnologías, y en especial de Internet, no hace sino facilitarlo e incrementarlo.

6. LA FACTURA ELECTRÓNICA

Entre los aspectos que más llaman la atención en la contratación electrónica de bienes y servicios se encuentra el de la facturación y su posibilidad de realizarla electrónicamente, así como los aspectos fiscales; parece que en este tipo de contratación pueda eludirse con mayor facilidad la presión fiscal incluso sea más sencilla la comisión de un fraude fiscal-, al tiempo que se plantean dudas sobre la aplicación de la política tributaria.

De otra parte, también hay que considerar que la facturación electrónica y su implicación fiscal, cuando la transacción ha sido realizada a través de una red –por ejemplo, por Internet–, puede estar afectando a dos o más Territorios, Países o Estados, con diferentes tipos de tributación e, incluso, con distintas políticas fiscales.

Las preguntas, de esta forma, surgen fáciles: ¿cuál será el país de tributación?, ¿existirá una doble tributación, incluso una doble imposición?, ¿es más fácil eludir la presión fiscal?

En otro orden de cosas, no debemos olvidar que la utilización de medios telemáticos en la contratación, y la creación y gestión de facturas por estos medios, facilita la ocultación de las operaciones, lo que puede significar, en la práctica, una forma de eludir tributaciones, o para modificar diferentes operaciones, simulando que se tratan de algunas diferentes y que se pueden introducir, de acuerdo con inconfesables intereses, en el lugar, transacción o entidad que convenga, dificultando su seguimiento.

Sabemos que los profesionales y empresarios tienen la obligación de expedir y entregar facturas, además de conservar una copia de las mismas durante un período determinado de tiempo correspondiente al plazo de prescripción del derecho que tiene la administración para indagar e inspeccionar en las deudas tributarias correspondientes a la transacción efectuada, y sus consecuencias o vinculaciones con otras operaciones, y así está establecido en el artículo primero del Real Decreto 1496/2003, de 28 de diciembre, por el que se aprueba el Reglamento por el que se regulan las obli-

gaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido [64] y que establece el deber de expedir y entregar factura que incumbe a los profesionales y empresarios, y que expresamente prevé la remisión y conservación de facturas por medios electrónicos, siempre y cuando se cumplan los requisitos establecidos en dicho Real Decreto, y en particular que cuando se vayan a remitir por tales medios el destinatario haya dado su consentimiento expreso y quede garantizada la autenticidad e integridad de la información así transmitida.

Con anterioridad a dicho Real Decreto y con respecto a la facturación telemática, el artículo 9 bis del Real Decreto 2402/1985 [65], artículo que fue introducido en diciembre de 1992, concedía validez a las facturas emitidas informáticamente, y transmitidas telemáticamente, al indicar que las facturas transmitidas por vía telemática a que se refiere el artículo 88.2 de la Ley del I.V.A., tendrán la misma validez que las facturas originales con el condicionante de que la factura emitida y recibida deberá ser idéntica, pero añade que la Administración Tributaria podrá, en cualquier momento, exigir, tanto al emisor como al receptor de la factura, su emisión en papel y en lenguaje legible.

Posteriormente, mediante el Real Decreto 80/1996, de 26 de enero, por el que se modifica el Reglamento del Impuesto sobre el Valor Añadido y el Real Decreto 2402/1985, se modificó este artículo 9 bis del Real Decreto 2402/1985, señalando que los empresarios y profesionales que quisieran utilizar el sistema de facturación telemática tenían que solicitar a la Agencia Estatal de Administración Tributaria:

"De autorización de su uso con una anticipación mínima de treinta días a su puesta en servicio".

Sistemas de intercambio de facturación telemática

En relación con la emisión de facturas electrónicas la Orden HAC/3134/2002, de 5 de diciembre [66], deroga, en virtud de su Disposición derogatoria única, la Orden de 22 de marzo de 1996 en la que se establecía un sistema de intercambio de facturación telemática junto con las obligaciones de cada uno de los intervinientes en dicho sistema.

La Orden HAC/3134/2002 establece en su artículo quinto la autorización de los sistemas de facturación electrónica, distinguiendo dos tipos de sistemas de intercambio electrónico de datos. Por un lado, el sistema de intercambio electrónico de datos basado en sistemas de firma electrónica avanzada que sean admitidos por la Agencia Estatal de Administración Tributaria y, por otro lado, se establecen otros sistemas de intercambio electrónico de datos autorizados por la Administración Tributaria.

En el primer caso, las autorizaciones de los sistemas de facturación electrónica y de su uso se entienden automáticamente concedidas si se utilizan los sistemas de firma electrónica avanzada admitidos por la Agencia Estatal de Administración Tributaria en función de las normas de aplicación del régimen de facturación vigentes y del Real Decreto 2402/1985, de 18 de diciembre, sobre el deber de expedir y entregar facturas por los empresarios y profesionales, en su redacción dada por el Real Decreto 80/1996, de 26 de enero.

En el caso de los empresarios o profesionales deberán ser titulares de un certificado electrónico de identificación en vigor y disponer de los mecanismos de producción y de verificación de firma de entre los admitidos por la Administración Tributaria.

En el segundo caso, si se desean utilizar otros mecanismos de intercambio electrónico de datos distintos de los basados en dispositivos de firma electrónica avanzada se debe solicitar al Departamento

[64] *Publicado en el Boletín Oficial del Estado número 286, de 29 de noviembre.*

[65] *Real Decreto 2402/1985, de 18 de diciembre, mediante el que se regula el deber de expedición y entrega de facturas por empresarios y profesionales.*

[66] *Orden HAC/3134/2002, de 5 de diciembre, sobre un nuevo desarrollo del régimen de facturación telemática previsto en el artículo 88 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, y en el artículo 9 bis del Real Decreto 2402/1985, de 18 de diciembre, publicada en el Boletín Oficial del Estado número 298, de 13 de diciembre, y desarrollada por Resolución 2/2003, de 14 de febrero, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre determinados aspectos relacionados con la facturación telemática, publicada en el Boletín Oficial del Estado número 51, de 28 de febrero.*

de Inspección Financiera y Tributaria de la Agencia Estatal de Administración Tributaria, en los términos del artículo 9 bis del Real Decreto 2402/1985, indicando los elementos que permitan garantizar la autenticidad de origen e integridad de contenido de las facturas. Una vez autorizado el sistema propuesto, los usuarios deben presentar una solicitud de uso del mismo ante el Director del Departamento de Inspección Financiera y Tributaria de la Agencia Estatal de Administración Tributaria, con una anticipación mínima de treinta días antes de su puesta en servicio. En la solicitud se indicarán los medios autorizados de autenticación, cuando se base en firma electrónica avanzada, o las especificaciones del sistema de intercambio electrónico de datos, en otro caso, utilizados.

7. EL USO DE LAS TIC EN EL ÁMBITO TRIBUTARIO

Ahora bien, también puede darse otro enfoque a la informatización de la Administración Tributaria, esto es, desde el punto de vista de la mejora de la eficiencia y de la participación del ciudadano en el cumplimiento de sus deberes tributarios. Así, si en distintos lugares hemos planteado las dificultades de seguimiento y control de la tributación electrónica, pasamos ahora a exponer el adelanto de la Administración Tributaria en relación con las posibilidades de actuación e interacción con el administrado.

Conforme a lo dispuesto en su página web (www.aeat.es) los servicios de la Administración tributaria electrónica se caracterizan por actualizar diariamente la información, disponibilidad de los servicios ofrecidos 24 horas al día, siete días a la semana, facilitar los certificados tributarios solicitados por Internet en un plazo máximo de cinco días, extender progresivamente el sistema de presentación de declaraciones por Internet a todos los modelos de declaración e incrementar paulatinamente los certificados tributarios que se pueden solicitar y obtener a través de Internet, por último fomentar la participación de organismos públicos, entidades, asociaciones y corporaciones empresariales, profesionales, sindicales y sociales, en la prestación de servicios personalizados por Internet con la finalidad de hacerlos accesibles a un mayor número de ciudadanos.

Entre los servicios que se ofrecen telemáticamente destacamos los de información *on line*, presentación de declaraciones a través de Internet en los correspondientes plazos de presentación durante las 24 horas del día, utilizando el certificado de usuario expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) o cualquiera de los certificados electrónicos expedidos por otros Prestadores de Servicios de Certificación que son admitidos por la AEAT como por ejemplo los del Consejo Superior de Cámaras. Dichos certificados electrónicos garantizan plenamente la seguridad y la confidencialidad de la transmisión a través de una red abierta como Internet. Este sistema permite simplificar y agilizar la tramitación posterior de las declaraciones, anticipando la devolución que se hubiera podido solicitar.

También ofrece la expedición de certificados tributarios, válidos ante otros organismos, previa solicitud del interesado en la oficina de la Agencia Tributaria correspondiente a su domicilio fiscal o, en el caso de las grandes empresas, en la respectiva Unidad de Gestión. Disponiendo que quienes tengan un certificado de usuario para la presentación de declaraciones a través de Internet pueden solicitar y obtener directamente determinados certificados por esta vía.

Otros son el Despacho aduanero de mercancías en las Aduanas, por medios telemáticos y en las instalaciones de importadores y exportadores autorizados. El formulario único válido para presentar solicitudes, plantear alegaciones, aportar documentación o dirigir cualquier comunicación a la Agencia Tributaria, disponible en las oficinas y en Internet. La presentación de determinados recursos de reposición y otras solicitudes de carácter tributario: devolución de ingresos indebidos, rectificación de errores aritméticos, materiales o de hecho, y rectificación de autoliquidaciones.

8. SUPUESTOS PRÁCTICOS

Partiendo de esta conclusión examinemos brevemente algunos supuestos prácticos que pueden plantearse en la actividad diaria:

a. Supuestos en los que se debe realizar una entrega de bienes

Debemos considerar dos circunstancias concretas:

a. *cuando deben ser objeto de expedición o transporte:*

   i. *Regla general:* la obligación de tributar nace en el lugar donde se encuentren los bienes al inicio de la expedición o transporte.

   ii. *Supuesto especial:* cuando la salida de la expedición o transporte se efectúe desde un Estado tercero, se considerará que el lugar de la entrega se halla en el Estado miembro de importación. Así, si se adquiere un bien a otro Estado y dicho bien resulta estar en un tercer Estado, el impuesto no se gravará desde el inicio de la expedición o transporte sino que, para evitar una doble imposición, se gravará desde el Estado que ha de importar el bien, es decir, con el que se realizó la correspondiente transacción de adquisición.

Veámoslo en un ejemplo: un empresario residente en España, adquiere un bien a una empresa francesa, residente en Francia, que tiene almacenados esos bienes en Italia. Será la empresa residente en Francia la que devengue el impuesto a la española sin que entre Italia y Francia se devengue I.V.A. porque si no estaríamos ante un mismo bien gravado por un mismo impuesto dos veces.

b. *cuando los bienes deben ser objeto de instalación o montaje:* en este caso el impuesto ha de gravarse en el lugar donde se realice la instalación o montaje. Pero si la instalación o montaje se efectúa en un Estado miembro distinto del proveedor, corresponde a este tercer Estado adoptar las medidas necesarias para evitar la doble imposición.

	Circunstancias	Reglas	Tributación de I.V.A.
ENTREGA DE BIENES	Expedición o transporte	Regla general	Estado donde se encuentre el bien al contratar
		Objeto situado en tercer Estado	Estado importador del bien
	Instalación o montaje	Regla general	Lugar donde se realice la instalación o montaje
		Instalación o montaje en un tercer Estado	Estado importador

b. En cuanto a las prestaciones de servicios

a. *Regla general:* se grava el impuesto en el lugar en que se encuentre la sede de la actividad del prestador o, en su defecto, el establecimiento permanente, el domicilio o residencia habitual.

b. *Servicios de telecomunicaciones y los efectuados por vía electrónica siempre y cuando se presten a personas establecidas fuera de la Comunidad[67] o a sujetos pasivos establecidos en la Comunidad miembro, pero fuera del país del prestador:* el impuesto se gravará donde se halle la sede de la actividad económica o, en su defecto, establecimiento permanente, domicilio o residencia habitual del destinatario del servicio.

[67] *Según la definición de Comunidad dada por la Directiva 77/388 y para el caso de España se corresponde con el interior del país exceptuando Canarias, Ceuta y Melilla. Por tanto, lo previsto en este estudio no será de aplicación a Canarias, Ceuta y Melilla.*

Los servicios realizados a través de vía electrónica se enumeran en el Anexo L de la Directiva 2002/38/CE[68] que establece la siguiente lista ilustrativa:

1. *El suministro y alojamiento de sitios informáticos, el mantenimiento a distancia de programas y de equipos*
2. *El suministro de programas y su actualización*
3. *El suministro de imágenes, texto e información y la puesta a disposición de bases de datos*
4. *El suministro de música, películas y juegos, incluidos los de azar o de dinero, y de emisiones y manifestaciones políticas, culturales, artísticas, deportivas, científicas o de ocio*
5. *El suministro de enseñanza a distancia*

Según esto, si una persona física o jurídica recibe la prestación de un servicio de estas características, no se va a gravar el impuesto en el lugar donde se encuentre el prestador del servicio sino que al ser un servicio cuyo consumo está destinado a la Unión Europea se gravará dentro de la misma.

A estos efectos, si a una persona, de un Estado miembro, se le suministra un servicio de telecomunicaciones por un empresario o profesional de fuera de la Comunidad en vez de considerarse como lugar del hecho imponible la sede de la actividad económica, establecimiento permanente, domicilio o residencia habitual del prestador se va a entender realizada la prestación dentro de la Comunidad, siempre y cuando la utilización y explotación del servicio se lleve a cabo dentro de la Comunidad.

Otra singularidad en los servicios de telecomunicación se produce cuando dichos servicios se prestan a personas que no tengan la consideración de sujetos pasivos y, en este sentido, los Estados miembros están facultados a invertir el lugar del hecho imponible por las razones mencionadas y, por tanto, cuando el lugar de las prestaciones de servicios se halle dentro o fuera del interior del país o de la Comunidad podrá modificarse en función del sitio donde se realice la utilización y explotación efectiva del servicio.

Por lo que, si una persona obtiene un servicio de telecomunicaciones que lo utiliza y explota fuera de la Comunidad, el impuesto ha de gravarse fuera. Y en el caso de que una persona utilice y explote el servicio en el interior del país el impuesto se gravará dentro de la Comunidad.

Respecto de los servicios efectuados por vía electrónica (reflejados en el Anexo L citado), se prevé una excepción en el supuesto de que sean prestados por sujetos pasivos establecidos fuera de la Comunidad a personas de un Estado miembro, que no tengan la consideración de sujetos pasivos, la prestación del servicio se va a localizar en el lugar en que la persona que no tenga la condición de sujeto pasivo posea su establecimiento, domicilio o residencia habitual. Por lo que, si una persona obtiene la prestación de un servicio, realizado por vía electrónica, proveniente de un empresario o profesional establecido fuera de la Comunidad el impuesto se va a gravar en el lugar en que esté establecido el destinatario del servicio.

El sistema de las prestaciones de servicios, ya sean servicios de telecomunicaciones o consistan en servicios efectuados por vía electrónica, se puede esquematizar en la tabla siguiente:

[68] *Directiva 2002/38/CE del Parlamento Europeo y del Consejo, de 7 de mayo, por la que se modifica temporalmente la Directiva 77/388/CEE respecto del régimen del impuesto sobre el valor añadido aplicable a los servicios de radiodifusión y de televisión y a algunos servicios prestados por vía electrónica, publicada en el Diario Oficial serie L, núm. 128, de 15 de mayo.*

PRESTACIÓN DE SERVICIOS

LUGAR DE REALIZACIÓN DEL HECHO IMPONIBLE	
COMO REGLA GENERAL	Sede de la actividad económica del prestador, su establecimiento permanente, domicilio o residencia habitual.

EXCEPCIÓN: Para los servicios de telecomunicaciones y los efectuados por vía electrónica

SUPUESTOS	LUGAR
Si se prestan a: • Personas de fuera de la Comunidad • Sujetos pasivos de la Comunidad pero fuera del país del prestador	Sede de la actividad económica, establecimiento permanente, domicilio o residencia habitual del **destinatario**

EXCEPCIÓN: Para los servicios efectuados por vía electrónica

Prestados • A personas que no tengan consideración de sujeto pasivo de un Estado miembro • Por sujetos pasivos de fuera de la Comunidad	Establecimiento, domicilio o residencia habitual de la **persona** que no tenga consideración de **sujeto pasivo**

EXCEPCION: Para los servicios de telecomunicaciones

Prestados: • A personas que no tengan la consideración de sujetos pasivos de un Estado miembro • Por sujeto pasivo de fuera de la Comunidad Inversión de la regla general	INVERSIÓN DE LA REGLA GENERAL	**Dentro de la Comunidad,** en vez de fuera, si la utilización y explotación se realizan dentro **Fuera de la Comunidad,** en vez de dentro, si la utilización y explotación se realizan fuera
Prestados a personas que no tengan la consideración de sujetos pasivos		**Dentro de la Comunidad,** en vez de fuera, si la utilización y explotación se realizan dentro

capítulo sexto

Protección de datos en la empresa

1. INTRODUCCIÓN

Actualmente las empresas no pueden prescindir, para llevar su gestión, de acudir a un tratamiento automático de la información utilizando la potencialidad de la informática e, incluso, de la informática más las comunicaciones. La gestión de los recursos, la prestación de servicios, la toma de decisiones, así como las funciones, entre otras, de planificación y control, obligan a manejar muchos datos, y esto no es posible sin su tratamiento mediante las Tecnologías de la Información y las Comunicaciones (TIC).

En muchos casos, los gestores de recursos ajenos se encuentran ante la necesidad del conocimiento de diferentes tipos de datos e informaciones de las personas para realizar con eficacia su gestión o controlar aquellos aspectos orientados al cumplimiento de objetivos de interés común.

El tratamiento automatizado de la información no está exento de riesgos y peligros entre los que se muestra como preferente atender al respeto debido a las personas ante el derecho fundamental de nueva creación que se ha dado en denominar "derecho fundamental a la protección de datos" [69].

Entenderemos por 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, en los límites de su intimidad".

Los archivos y registros de datos de personas –con las que la empresa mantiene una relación contractual, laboral, de cliente, proveedor, económica, social u otras–, se encuentran, generalmente, en soportes automatizados, o susceptibles de tratamiento automatizado, a los que se puede acceder mediante un programa de recuperación de información por determinados parámetros, bajo la forma y estructura conocida de las bases de datos, lo que facilita su recuperación y consulta y proporciona

[69] *La Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional, estimando el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo, contra los artículos 21.1 y 24.1 y 2 de la LOPD, claramente indica 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 ..." (último párrafo del Fundamento Jurídico 5). Así como también lo señala el artículo 8 de la Carta de los derechos fundamentales de la Unión Europea de 7 de diciembre de 2000 (2000/C 364/01), cuando dice: "Artículo 8. Protección de datos de carácter personal: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

una agilidad y dinámica a su tratamiento[70]; los parámetros de recuperación suelen ser los datos identificativos de la persona -nombre, apellidos, fecha y lugar de nacimiento, etc.- y algún número o código asociado que puede ser utilizado -mal utilizado- para el intercambio de información y cruce de datos no autorizado.

Este tratamiento de datos, con la posibilidad indicada de cesión[71] de los mismos a terceros o de utilización del resultado del tratamiento, atenta, en principio, contra una elemental protección a la intimidad de la persona y este es, en un primer aspecto, el derecho a proteger: el de la intimidad.

No podemos olvidar que los datos que tratamos en la empresa no son nuestros; son de sus titulares, de los interesados o afectados como los denomina la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

Es por ello que, cumpliendo con la normativa vigente, se pueden tratar los datos cuando ese tratamiento sea lícito pero teniendo en cuenta que estamos haciendo un tratamiento sobre datos que son de otros y que debemos respetar, consecuentemente, todos los principios y derechos que sobre ellos contempla la ley.

Es frecuente escuchar a responsables de empresas que dicen que tienen ficheros de datos suyos que les ha costado mucho tiempo conseguir. Tendrán ficheros de datos y será cierto que les habrá costado mucho tiempo conseguirlos, pero también es cierto que los datos no son suyos, son de sus titulares, y deberán ser tratados con la conciencia de que estamos trabajando sobre "algo que no es nuestro" y, por tanto, debe ser respetado, al menos en la forma que marca la licitud del tratamiento en las normas correspondientes.

Y esa forma de tratar los datos, que debe tener en consideración el titular del fichero, la empresa, se debe hacer considerando las tres fases en las que se estructura el tratamiento de datos de carácter personal y que es necesario su exposición para mejor comprender y aplicar la correspondiente normativa; interpretar las normas sobre protección de datos y fijar las obligaciones del titular del fichero se debe hacer teniendo en consideración los tres momentos o fases en que se desarrolla, o puede desarrollar, el tratamiento automatizado de datos de carácter personal y que son:

1. El momento de recabar los datos, bien sea directamente del interesado o de un tercero[72], en el que tiene gran importancia su licitud y lealtad[73], con las características de conocimiento y, en su caso, consentimiento del afectado;

2 El momento del tratamiento de los datos, que pueden ser cruzados y relacionados en forma automática junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer, y

3. El momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento, conocida ésta última como "cesión o comunicación de datos", en la que, al igual que en la recogida y en el tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular.

---

[70]Lo que representa un peligro, pues las facilidades de consulta y rapidez de acceso a la información permiten también la interconexión de bases de datos y la posibilidad de procesamiento, con una facilidad de cruce de los mismos y de localización de un perfil determinado, respecto a informaciones o modelos seleccionados.

[71]Definida en la letra i) del artículo 3 de la Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado".

[72]La vigente Ley de protección de datos (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, muestra con fuerza esta obligación de informar al afectado ya sea cuando los datos se recaben del propio interesado, que deberá ser informado en ese momento, o cuando se recaben de terceros, que deberá ser informado (art. 5.4), "de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad".

[73]El concepto de lealtad que al figurar en una ley puede parecer, y lo es, un concepto jurídico indeterminado, tiene gran importancia por la referencia expresa y concreta que a él hace la ley española de protección de datos y, con mayor fuerza, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE), publicada en el Diario Oficial, serie L, núm. 281, de 23 de noviembre.

Estos tres momentos deben estar siempre presentes en el estudio de los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer sus derechos.

2. NORMATIVA

La norma básica que debe conocer toda persona que trate datos de carácter personal es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En esta norma se reconoce a los ciudadanos unos derechos en el tratamiento de sus datos personales, estableciendo determinadas garantías que obligan a los titulares de ficheros[74] y, consecuentemente, nace la necesidad de realizar y establecer un entorno organizativo, con importantes repercusiones jurídicas, para cumplir con los principios contemplados en la norma y respetar el ejercicio de sus derechos por los ciudadanos.

Deben ser respetados los principios de protección de datos que se contemplan en la LOPD y organizar el flujo lógico de la información en la empresa de forma que sea fácil, y seguro, no solamente cumplir con lo establecido en la norma, sino también poder comprobar que se realiza el tratamiento lícito, adecuado, que permita poder atender todos los derechos de los ciudadanos titulares de datos.

Esta norma principal se acompaña de dos Reglamentos que, si bien no la desarrollan directamente a ella, porque corresponden a desarrollos referentes a su norma antecedente, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), permanecen vigentes en tanto en cuanto no la contradigan ni se produzca un desarrollo reglamentario posterior[75]. Y estos dos Reglamentos son el aprobado por Real Decreto 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, en adelante, Real Decreto 994/1999 o Reglamento de medidas de seguridad, y el Real Decreto 1332/1994, de 20 de junio que desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, en adelante, el Real Decreto 1332/1994 o el Reglamento.

3. ÓRGANO DE CONTROL

La Agencia Española de Protección de Datos (AEPD) es el órgano de control de la Protección de datos, tiene calidad de ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada y actúa con total independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Creada por la derogada LORTAD[76] y regulada en la vigente LOPD, la Agencia se muestra como la instancia a la que pueden acudir los afectados para ser tutelados en el ejercicio de sus derechos[77]. Existiendo actualmente, además de la Agencia Española de Protección de Datos, tres Agencias autonómicas, en Madrid, en Cataluña y en el País Vasco.

En el ejercicio de sus funciones públicas, y en defecto de lo que dispongan la LOPD y sus disposiciones de desarrollo, indica el apartado segundo, del artículo 35, de la LOPD, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

---

[74] A cualquier empresa que tenga o mantenga datos personales en un soporte automatizado o susceptible de tratamiento automatizado.

[75] Así se desprende de la Disposición Transitoria tercera de la LOPD.

[76] El apartado primero del artículo 34 de la LORTAD indicaba sobriamente "se crea la Agencia de Protección de Datos".

[77] Pero ello no quiere decir que deba presentarse como institución atemorizante dispuesta a sancionar e imponer fuertes multas a los titulares de los ficheros que, solamente por errores cometidos, aparezcan señalados por los afectados. Como órgano de control del cumplimiento de la ley deberá ejercer sus funciones al servicio de los ciudadanos y de la sociedad en su conjunto, cumpliendo sus fines de apoyo y desarrollo de una normativa, así como de cauce y ayuda interpretativa, pero no convirtiéndose en ese fiscalizador atemorizante, con exceso de poder, que impida, incluso, el desarrollo de elementos tecnológicos que podrían tener una función de servicio al desarrollo del hombre, situándonos, otra vez más, en posturas de retroceso o, al menos, de imposibilidad de desarrollo con los mismos parámetros que otros países de nuestro entorno socio-económico.

La Agencia la dirige el Director, quien ostenta también su representación, que será nombrado de entre quienes componen el Consejo Consultivo (art. 36) *"mediante Real Decreto, por un período de cuatro años",* teniendo la consideración de *"alto cargo".*

La Ley regula también el funcionamiento y las funciones de la Agencia y de su Director, entre las que señalamos, por ser de mayor interés en este trabajo, atender las peticiones y reclamaciones formuladas por las personas afectadas, proporcionar a las personas información acerca de sus derechos sobre esta materia, ejercer la potestad inspectora y la sancionadora en los términos previstos en la Ley, ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la Ley, ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos y, otras que tienden a velar por el cumplimiento de la legislación sobre protección de datos (art. 37) y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, cancelación y oposición.

Integrado en la Agencia, se encuentra el Registro General de Protección de Datos donde serán objeto de inscripción (art. 39), los ficheros de que sean titulares las Administraciones Públicas, cuando sea competente una Agencia de Protección de Datos autonómica, y los ficheros de titularidad privada.

Conviene destacar un ciclo de actuaciones administrativas que, en número de tres, configuran potestades, bien de la propia Agencia Española de Protección de Datos, bien de su Director, que distinguen y marcan claramente la línea operativa que en la práctica sirve como instrumento de control del cumplimiento de la Ley por el titular del fichero.

Nos referimos, en primer lugar, a la potestad inspectora, regulada en el artículo 40[78], que otorga a los funcionarios que ejerzan la inspección la consideración de autoridad pública en el desempeño de sus cometidos, facultándoles para solicitar la exhibición o el envío de documentos o de datos, así como para inspeccionar los equipos físicos y lógicos utilizados para el tratamiento accediendo a los locales donde se hallen instalados.

En segundo lugar, la LOPD otorga, al Director de la Agencia Española de Protección de Datos, potestad para inmovilizar los ficheros[79] en los casos en que el titular del mismo no atienda el requerimiento para cesar en la utilización o cesión ilícita de los datos.

Y, por último, la potestad sancionadora que, sin duda, constituye en la práctica el método más seguro para hacer cumplir a los reticentes y para una más eficaz protección de los derechos de los afectados. En la propia Exposición de Motivos de la derogada LORTAD se contemplaba la potestad sancionadora como lógico correlato de la función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias.

En este sentido, entre las funciones de la Agencia Española de Protección de Datos, el apartado g) del artículo 37 de la Ley, contempla la de *"ejercer la potestad sancionadora en los términos previstos por el título VII de la presente Ley".*

4. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El problema surge con el tratamiento del dato y las conclusiones que se puedan obtener al asociarle a una persona determinada; esta subjetivación y valoración es la que contiene una potencial agresividad al derecho fundamental de la persona.

---

[78]El primer apartado del artículo 40 de la LOPD indica que "Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos".

[79]Potestad que, bajo el epígrafe de "potestad de inmovilización de ficheros", se encuentra contemplada en el artículo 49 de la Ley.

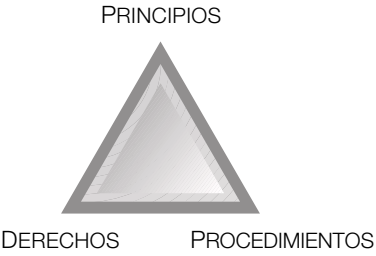
En principio, no se puede tratar ningún dato de carácter personal sin el consentimiento de su titular, interesado o afectado como le llama la Ley. Por tanto se podrán tratar todos aquellos datos para los que el titular de los mismos haya prestado su consentimiento salvo que concurra alguna excepción a esta necesidad de consentimiento como trataremos más adelante.

Es por tanto el titular de los datos el único que, como teoría general, puede decidir cuándo, dónde, cómo y por quién se tratan sus datos de carácter personal; y, además, con un derecho que ha sido elevado a la calidad de derecho fundamental.

Es así que, una vez conocidos qué datos se pueden tratar, pasaremos a ver en qué forma se deben tratar.

Los datos se deben tratar en la forma que queda especificada en la LOPD y que, resumida, consiste en contemplar los principios que figuran en el Título II[80] de la Ley y facilitar el ejercicio de los derechos de los ciudadanos mediante una adecuación de las normas de actuación en la empresa a lo que viene contemplado en el Título III[81] de la citada norma.

Esto es, no es suficiente contar con el consentimiento del titular del dato para poder proceder a su tratamiento, sino que, además, hay que adecuar ese tratamiento al respeto de los principios contemplados en la Ley y a facilitar el ejercicio de los derechos por el ciudadano.



Cabe estructurar el análisis y estudio de la protección de datos, siguiendo al Profesor Davara, 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. Es por ello que, de una forma práctica y orientada a esta adecuación de métodos y procedimientos en la empresa, pasamos a exponer los principios y derechos de la protección de datos.

5. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Los principios, contemplados en el Título II de la LOPD, artículos 4 a 12, marcan las exigencias en el tratamiento de datos para que sea lícito en las tres fases que hemos mencionado. Los principios de la protección de datos deben ser considerados íntegramente tanto al recabar los datos, como al someterles a tratamiento, como al utilizar los resultados del tratamiento o, en su caso, comunicar o ceder los datos a terceros.

Lo mejor que se puede recomendar a una empresa cuando quiere saber cómo debe cumplir con la normativa sobre protección de datos, es decirle que analice el flujo lógico de la información en la entidad y compruebe que en los tres momentos o fases del tratamiento se cumplen los principios de la protección de datos contemplados en los artículos 4 a 12 de la LOPD, desde la propia calidad de los datos

[80] *El Título II de la LOPD, bajo el epígrafe principios de la protección de datos, establece los principios de: calidad de los datos (art. 4), información en la recogida de datos (art. 5), consentimiento (art. 6), datos especialmente protegidos (art. 7), datos relativos a la salud (art. 8), medidas de seguridad (art. 9), deber de secreto (art. 10), cesión o comunicación de datos (art. 11) y acceso a los datos por terceros (art. 12).*

[81] *El Título III de la LOPD, bajo el título derechos de las personas, contempla los derechos de: impugnación de valoraciones (art. 13), consulta al Registro General de Protección de Datos (art. 14), acceso (art. 15), rectificación y cancelación (art. 16) e indemnización (art. 19).*

hasta, en su caso, el acceso a datos por cuenta de terceros mediante la figura del encargado del tratamiento.

Es así como comenzaremos analizando los principios contemplados en la Ley; pero no lo vamos a hacer en el orden de los artículos de la norma sino en un orden lógico que permita en la práctica seguir con aprovechamiento su utilización e implementación; esto es, recomendamos seguir el orden lógico que exponemos para poder comprender de forma práctica cuáles son los principios y la forma de cumplirlos por el titular responsable del fichero o del tratamiento (la empresa).

Es así que empezamos por el denominado principio del consentimiento por considerarle, como ya hemos hecho referencia, el eje central de protección en nuestra norma.

a. El consentimiento del titular de los datos

La teoría general sobre la que gira nuestra norma de protección de datos es el llamado "principio del consentimiento" que podemos resumir, como ya hemos indicado, diciendo que el ciudadano es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o se dan a conocer sus datos a terceros; esto es, el afectado tiene que otorgar su consentimiento para que se pueda realizar un tratamiento de sus datos de carácter personal; dicho de otra forma, no se pueden tratar datos de carácter personal sin el consentimiento de su titular (del titular de los datos).

Pero, este principio general tiene sus excepciones. Veamos:

> *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*

indica el apartado primero del artículo 6 de la LOPD, pero, a continuación (apartado segundo), refiere una serie de casos en los que no es preciso el consentimiento para el tratamiento de los datos, exponiendo, vía excepción, que

> *"2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

Analizando este apartado, y desde la óptica que nos ocupa en este trabajo[82], debemos señalar que las excepciones que aquí se contemplan a la exigencia del consentimiento son tres:

1. Cuando una ley así lo disponga.

2. Cuando los datos se recojan de fuentes accesibles al público[83]: en este caso que no haga falta consentimiento no quiere decir que no sea necesario el conocimiento y, por consiguiente, habrá que infor-

[82] *Se trata de un trabajo referido exclusivamente a ficheros cuyos titulares son las empresas, esto es, ficheros de titularidad privada. La LOPD hace una distinción contundente entre ficheros de titularidad pública y ficheros de titularidad privada, llegando incluso a dedicar dos capítulos diferentes (capítulo primero del Título IV, bajo la rúbrica de ficheros de titularidad pública y capítulo segundo del mismo Título IV, bajo la rúbrica de ficheros de titularidad privada), para separar características en su regulación; este trabajo se centra solamente en los ficheros de titularidad privada de las empresas e, independientemente de las críticas que nos merece esta clara diferenciación, centraremos la atención solamente sobre ellos.*

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

mar al interesado en la forma que prescribe el artículo 5 de la LOPD sobre que se está realizando el tratamiento de sus datos y, naturalmente, el fichero, los datos recabados y el tratamiento que se efectúe, deberán ser adecuados a lo especificado en la norma.

3. Cuando los datos de carácter personal se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. Si entramos en el análisis de "la necesidad" exigida para el mantenimiento de las relaciones o para el cumplimiento del contrato, nos encontramos, como en todos los casos en que se manejan conceptos jurídicos indeterminados, con problemas de interpretación y, en particular, referente a esta cuestión, consideramos que debía existir, vía Instrucción, algún pronunciamiento de la Agencia Española de Protección de Datos.

En otro orden de cosas, podríamos expresar diversas teorías sobre si el consentimiento a que se refiere el artículo 6 de la LOPD, puede ser tácito y, en caso de que deba ser expreso, si debe ser por escrito.

Nuestra opinión es que el consentimiento, dependiendo de los casos de que se trate y la regulación que de él hace la Ley, puede ser en unos casos tácito, en otros expreso y, por último, para una categoría especial de datos, tiene que ser expreso y por escrito[84].

Señalar también que en el caso de que sea necesario el consentimiento, éste puede ser revocado; el apartado tercero del referido artículo 6, indica que:

> *"El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos".*

b. La calidad de los datos

Independientemente de lo que ya hemos expresado sobre la necesidad del consentimiento para recoger y tratar datos de carácter personal, y las excepciones al mismo, los datos que se recaben deben ser pertinentes y adecuados al fin que se pretenda, además de que no podrán permanecer en el fichero por tiempo mayor al necesario para cumplir con la finalidad para la que se obtuvieron.

La calidad de los datos, fuente de múltiples conflictos interpretativos, se encuentra reflejada en el artículo 4 de la LOPD que, con una amplia redacción en siete apartados, podemos resumir indicando que la información, o los datos que se recaban o que se registran en un fichero, debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales[85] y, añadimos nosotros, leales[86].

Ello exige, girando sobre el concepto de pertinencia de los datos, de acuerdo con el ámbito y la finalidad para los que se hayan obtenido, que vaya acompañado de su exactitud y su actualización[87].

La utilización de acuerdo con el fin para el que fueron obtenidos –adecuación al fin–, junto con la cancelación y sustitución de oficio en determinados supuestos –debido a su inexactitud total o parcial– y el almacenamiento de forma que el titular pueda ejercer su derecho de acceso, son los complementos que garantizan la calidad exigida por la norma.

---

[84]La LOPD al exigir el consentimiento lo hace de una forma genérica y, por lo tanto, cabe perfectamente el consentimiento tácito; cuando la Ley quiere que el consentimiento sea expreso lo declara con nitidez, llegando al extremo de exigir el consentimiento "expreso y por escrito" cuando se refiere al tratamiento de los datos que denomina "especialmente protegidos" y, en particular (apartado 2, del artículo 7), los que "revelen la ideología, afiliación sindical, religión y creencias". De igual forma, cuando se trata de "cesión de datos", se habla solamente de consentimiento sin exigencia de que sea expreso (así, apartado 1, del artículo 11). Que el consentimiento puede ser tácito se remacha también en el artículo 44 cuando al exponer los tipos de infracciones, indica (apartado 3) que son infracciones graves "c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible", con una agravación en la calificación de la infracción, (apartado 4) que califica de muy grave "c) Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado".

[85]Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos, indica el séptimo apartado, del artículo 4 de la Ley.

[86]Los comentarios a la interpretación del término "lealtad" los realizamos en el apartado 7.b, y a ese lugar nos remitimos.

[87]Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, reza el tercer apartado del citado artículo 4 de la ley; pero, ¿qué debemos entender por puestos al día?; en muchas ocasiones, dificultades operativas y de gestión, incluso problemas de comunicación ajenos a nuestra voluntad, impiden la "puesta al día" de los datos.

De esta forma, a tenor de lo que establece la Ley, cuando los datos registrados sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, existiendo también la obligación de cancelarlos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

c. La información al recabar los datos

Es un principio general de protección de datos que todo ciudadano tiene derecho a conocer la información almacenada sobre sí mismo.

Cuando se recaben datos de una persona para ser utilizados mediante un tratamiento informático, o mantenerlos en un soporte susceptible de tratamiento automatizado, se debe realizar de una forma legal y leal; ello incluye que el afectado sea informado –de modo expreso, preciso e inequívoco, indica el primer apartado del artículo 5 de la LOPD–, de la finalidad de la recogida y de los destinatarios de la información, advirtiéndole si tiene o no obligación de contestar a las preguntas que se le realizan y de cuáles pueden ser las consecuencias en el caso de que se niegue a contestar o a proporcionar los datos.

Habrá que informarle también del derecho que tiene de ejercitar el acceso al fichero para saber los datos que de él se mantienen y, en su caso, exigir la rectificación o cancelación de los mismos cuando sean inexactos, obsoletos o no adecuados al fin perseguido. Asimismo, tendrá que indicarse la posibilidad de ejercitar el derecho de oposición[88] al tratamiento de datos, para aquellos casos en los que proceda. Como es natural, para que pueda ejercer sus derechos, se deberá notificar también al afectado sobre la identidad y dirección del responsable del fichero.

La LOPD distingue que los datos hayan sido recabados, o no, del propio interesado, señalando en el apartado cuarto, del artículo 5, que

> *"cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo*[89]*".*

d. Los llamados datos sensibles

La LOPD establece unas categorías de datos que deben ser objeto de especial protección[90]; es por ello que, en referencia directa al que hemos denominado principio del consentimiento, establece una excepción *sui generis* en el artículo 7.

El consentimiento del afectado, como ya hemos indicado, es necesario para recabar y tratar datos de carácter personal, "salvo que la ley disponga otra cosa"; pero este consentimiento puede ser tácito[91]; sin embargo, cuando se trata de los datos que el artículo 7 considera especialmente protegidos y a los que hacemos referencia, el consentimiento debe ser expreso, indicando, como mayor garantía, que en el caso de los datos a que se refiere el artículo 16.2. de la Constitución[92] y los datos referentes a la afiliación sindical, el consentimiento debe ser, además de expreso, por escrito.

---

[88] *El derecho de oposición es un derecho nuevo en la LOPD, como consecuencia de la transposición de la Directiva 95/46/CE, que no tiene desarrollo reglamentario aún y que se encuentra recogido en el artículo 6.4 de la LOPD, dedicado al consentimiento.*

[89] *Se refiere en concreto a la siguiente información, apartado primero del artículo 5 de la LOPD, "a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información"; "d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición", y "e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

[90] *En términos generales diremos que se trata de los datos referentes al origen racial, a la salud y a la vida sexual por un lado y, por otro lado, a la ideología, afiliación sindical, religión y creencias.*

[91] *Es necesario insistir en que, aun siendo válido el consentimiento tácito, acudiremos a él solamente en los casos en que sea absolutamente necesario, debido a las dificultades de prueba que tiene.*

[92] *Que son los que se refieren a la ideología, religión y creencias.*

Se completa la garantía sobre los datos que se refieran a la ideología, religión y creencias, y la exigencia de protección especial, al indicar el artículo que, además

> *"Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo".*
>
> *Al tiempo que se prohíbe la creación de ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.*

e. Las medidas de seguridad

El artículo 9 de la LOPD, desarrollado reglamentariamente por el Real Decreto 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 (en adelante, como hemos indicado, Real Decreto 994/1999 o Reglamento de medidas de seguridad) establece que el responsable del fichero y, en su caso, el encargado del tratamiento deben adoptar las medidas de índole técnica y organizativas necesarias con el fin de garantizar la seguridad de los datos personales objeto de tratamiento, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Consiste en garantizar la confidencialidad e integridad de la información que se trata en los sistemas de información. En relación con la aplicación de las medidas de seguridad no vamos a extendernos más aquí remitiéndonos a un apartado posterior en el que se realiza un análisis exhaustivo de las mismas.

f. El deber de secreto

La LOPD, en su artículo 10, impone al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de datos la obligación de secreto profesional respecto de los datos tratados así como el deber de guardarlos, aún una vez finalizadas sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo. En relación con este deber de secreto nos remitimos al apartado de obligaciones del responsable del fichero en el que se desarrolla más ampliamente este principio.

g. La cesión o comunicación de datos

La cesión de datos es un punto conflictivo cuando se trata de proteger la llamada "privacidad"; de una parte, porque cediendo los datos a otros ficheros se posibilita el cruce de los mismos, aplicando con toda intensidad las posibilidades de tratamiento de la información que posee la informática y, de otra parte, porque la propia cesión facilita la utilización de los datos para un uso que no es el mismo para el que se habían recabado.

Respecto a la cesión de los datos, se detallan, en el artículo 11 de la Ley, las condiciones en las que podrán o no ser cedidos, indicando que no se podrán ceder los datos de carácter personal objeto de tratamiento automatizado más que:

> *"para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario"*

y, salvo que la Ley prevea otra cosa, o se trate de datos recogidos de fuentes accesibles al público, con el previo consentimiento del afectado o interesado.

Es, por tanto, necesario el consentimiento del afectado. Consentimiento que puede ser revocado y que será nulo cuando la información que se facilite al interesado no le permita conocer la finalidad a la que se destinarán los datos o el tipo de actividad de aquél a quien se pretenden comunicar; por tanto, se trata de un consentimiento específico para un cesionario también específico, determinando con claridad la finalidad de la cesión que se consiente.

No se indica que este consentimiento deberá ser escrito, ni revestir un formalismo determinado, de donde podemos deducir que puede ser tácito[93], siempre que podamos de él determinar con claridad la finalidad de la cesión que se consiente.

No será necesario el consentimiento, dice el apartado segundo del artículo 11:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

h. El encargado del tratamiento

Esta figura del encargado del tratamiento[94] que, por sí misma y en su definición, está recogida de una manera clara y diáfana, encuentra alto grado de complicación en la regulación que de su relación con el titular del fichero hace el artículo 12 de la Ley y que, sin duda, trae múltiples discusiones e interpretaciones en su adecuación práctica.

Termina el Título II de la LOPD, relativo a los principios de la protección de datos, con este artículo, que, como ya hemos referido, resulta polémico, en el que se establecen los requisitos para que el acceso a los datos por cuenta de terceros no sea considerado como comunicación o cesión, regulando la figura, ya citada, del "encargado del tratamiento".

Se indica en la norma que los tratamientos que se realicen por cuenta de terceros tendrán que figurar en un contrato que deberá constar por escrito *"o en cualquier otra forma que permita acreditar su celebración y contenido",* en el que se establecerán todas las características del tratamiento y se destacará expresamente que no se podrá comunicar estos datos, ni tan siquiera para su conservación, a terceros, con lo que queda totalmente prohibida la subcontratación.

La práctica y, expresado en otros términos, la necesidad y utilización real de esta figura, debe permitir el acceso a los datos, con una referencia en el contrato, y la consiguiente autorización por el titular del fichero, a aquellas personas a las que se podrá encargar un tratamiento específico; decimos, como aclaración, que, en nuestra opinión, si el titular del fichero autoriza en el contrato al que se refiere este artículo 12, a la contratación con un tercero determinado y específico, de unos también deter-

[93] *Para no provocar errores, insistimos en que el consentimiento tácito es válido siempre que la Ley no diga otra cosa (como es el caso de los datos especialmente protegidos), pero, volvemos a insistir, no es recomendable el consentimiento tácito por las dificultades de prueba que tiene. Hay que acudir al consentimiento tácito solamente en los casos en que sea absolutamente necesario.*

[94] *Al que en la letra g) del artículo 3 de la LOPD se le define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

minados y específicos tratamientos, estos no podrán ser considerados como subcontratación y tendrán cabida en la regulación de este artículo no tratándose, por tanto, de una comunicación o cesión.

6. DERECHOS DEL INTERESADO

Los principios se quedan en meras declaraciones teóricas si no tuvieran a su lado la posibilidad del ejercicio de unos derechos por el ciudadano que dieran contenido y efectividad práctica a esos principios.

De esta forma estamos obligados a decir que la empresa titular del fichero o del tratamiento no cumple solamente con tratar los datos de carácter personal respetando todos los principios recogidos en la norma sino que, además, es necesario que permita y facilite el ejercicio de los derechos por el interesado. Es decir, se debe estructurar un procedimiento lógico-administrativo que facilite el ejercicio de los derechos de acceso, rectificación, cancelación de los datos y oposición al tratamiento en la forma en que la LOPD contempla que pueden ser ejercidos y dentro de los plazos que figuran en la norma.

a. El derecho de impugnación de valoraciones

Nos referiremos en primer lugar al derecho de impugnación del interesado de determinados actos, cuando su fundamento sea un tratamiento automatizado de sus datos destinado a evaluar determinados aspectos de su personalidad, que se encuentra contemplado en el apartado segundo del artículo 13 de la norma que, bajo el epígrafe de "impugnación de valoraciones", expresa que:

> *El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.*

Es difícil entender esa limitación del texto a su "único fundamento", ya que se puede suponer que si la valoración de su comportamiento ha sido producto de analizar en conjunto datos de carácter personal sometidos a un tratamiento automatizado, por ejemplo, y datos de carácter personal sometidos a un estudio manual[95], ya no es posible, de acuerdo con la redacción de este artículo, impugnar los actos a los que se refiere. Será sencillo, por tanto, fundamentar en forma mixta, mediante un tratamiento automatizado y otro no, para poder eludir la impugnación del acto. Un ejemplo en el que puede darse el ejercicio de este derecho es el de la concesión de una tarjeta de crédito, en la que previamente se analiza la situación financiera del solicitante.

b. El derecho de consulta al Registro General de Protección de Datos

No cabe duda de que uno de los derechos del afectado es ser informado en la recogida de datos y, naturalmente, se convierte en obligación del titular del fichero, o de la persona o entidad que recaba los datos, informarle de modo expreso, preciso e inequívoco, en la forma y con las características que ya hemos indicado.

Pero el derecho de consulta al Registro General de Protección de Datos contemplado en la Ley (artículo 14), es el del afectado a recabar del Registro General de Protección de Datos, la información tendente a conocer si existen y cuáles son los ficheros de datos de carácter personal, consulta que realizará tantas veces como tenga interés siendo el Registro General de Protección de Datos "de consulta pública y gratuita". Esta información puede obtenerse a través de la dirección en Internet de la Agencia Española de Protección de Datos (www.agpd.es).

[95] *Un estudio no sometido a operaciones técnicas, de acuerdo con la definición de tratamiento de datos que contempla el apartado c), del artículo 3, de la LOPD.*

c. El derecho de acceso

El afectado puede dirigirse al titular del fichero para conocer los datos que sobre él tiene registrados. Este es el sentido y fundamento del denominado "derecho de acceso".

En la práctica es mediante este derecho como el afectado obtiene, o debe obtener, una información exacta y veraz sobre sus datos de carácter personal que se encuentran en el fichero de nuestra empresa o, en su caso, información sobre que el fichero no contiene ningún dato de carácter personal sobre él mismo[96].

Este derecho puede ser ejercido por el ciudadano en intervalos no inferiores a doce meses, esto es, solamente lo podrá ejercer una vez cada doce meses, excepto que exista causa justificada (interés legítimo, dice la LOPD), que indique una periodicidad menor, o por la cual el afectado pueda ejercer en períodos de tiempo inferiores su derecho de acceso.

El ejercicio del derecho de acceso está contemplado en la LOPD y en el Reglamento que establece el procedimiento para llevarle a cabo; no obstante, la Instrucción 1/1998 de la Agencia Española de Protección de Datos[97] destaca algunas características vía interpretativa que debemos señalar:

1. El responsable del fichero tiene obligación de contestar a la solicitud del derecho de acceso aunque en el fichero no se encuentren, ni nunca se hayan encontrado, datos de la persona que solicita la información[98].

2. En la respuesta que se envíe al afectado como consecuencia del ejercicio de su derecho de acceso, se deberá emplear cualquier medio que acredite el envío y la recepción[99].

3. El responsable del fichero debe actuar diligentemente llegando incluso a tener una obligación de "hacer", consistente en apoyar al afectado para que pueda subsanar los defectos que tuviera su petición[100].

d. Los derechos de rectificación y de cancelación

El afectado, en el caso de que los datos sean inexactos, o cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados, posee el derecho de rectificación o, en su caso, el derecho de cancelación; si los datos que se encuentran en un fichero son inexactos, incompletos o no existiera, por el motivo que fuera, derecho a su registro por parte del titular del fichero, el afectado podrá ejercer su derecho de rectificación o su derecho de cancelación[101].

El derecho a exigir que aquellos datos inexactos, incompletos o que hubieran dejado de ser pertinentes o adecuados para la finalidad para la que hubieran sido registrados, sean rectificados o cancelados se encuentra recogido en la Ley (art. 16) indicando que:

> *"El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días[102]".*

---

[96] *Indica el apartado primero del artículo 15 de la LOPD, que "el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".*

[97] *Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Publicada en el Boletín Oficial del Estado núm. 25, de 29 de enero. Aunque debe entenderse derogada, por ser anterior a la LOPD, permite conocer el criterio interpretativo de la Agencia Española de Protección de Datos.*

[98] *El apartado cuarto de la norma primera de la Instrucción 1/1998, indica que "el responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción".*

[99] *No se entiende con facilidad qué se debe interpretar como acreditar la "recepción" ya que ésta no depende del responsable del fichero y, por tanto, si la persona que la debe recibir se niega a hacerlo será imposible acreditar dicha recepción; entendemos que lo que se quiere decir es que se pueda acreditar la recepción o el intento de entrega, aunque no se haya logrado que la reciba el afectado.*

[100] *El apartado cuarto, de la norma primera de la Instrucción 1/1998, en su último párrafo, indica que "el responsable del fichero deberá solicitar la subsanación" en el caso de que la solicitud no reúna los requisitos especificados en la propia Instrucción y, por lo tanto, no sea atendible.*

[101] *El apartado segundo del artículo 16 de la Ley, indica que "Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos"*

[102] *Estos diez días han de entenderse y computarse, en el caso de los ficheros de titularidad privada, como días naturales, según la interpretación establecida por el Director de la Agencia Española de Protección de Datos con base en lo dispuesto en el apartado 2 del artículo 5 del Código Civil que dispone que "en el cómputo civil de los plazos no se excluyen los días inhábiles".*

Es así como los datos cuyo tratamiento no se ajuste a lo especificado en la Ley y, en particular, los datos que resulten ser inexactos o incompletos, serán rectificados o, en su caso, cancelados, debiendo comunicar el responsable del fichero esta circunstancia, con expresa indicación de los datos rectificados o cancelados, a todos aquellos a los que les hubiese cedido la información.

Cabe destacar que la cancelación no supone el borrado de los datos, sino su bloqueo; la figura del bloqueo, discutida y alarmantemente no entendida, por fin, tiene su respaldo en el propio texto de la norma.

La cancelación no puede exigir el borrado total y absoluto de los datos, aunque sea necesario el bloqueo con todas las características de seguridad que le deban acompañar; de otra forma, nos encontraríamos ante la extraña situación de que el borrado total de los datos no permitiría atender otras obligaciones, por no existir ya rastro alguno sobre los datos, como pueden ser los requerimientos realizados por los Jueces o Tribunales, o por la propia Administración, y teniendo en cuenta, además, que el responsable del fichero está obligado a atender las propias responsabilidades nacidas del tratamiento de los datos que exijan que no sean borrados, sino bloqueados, y cuya posibilidad ya queda recogida en el texto del artículo 16 de la LOPD[103].

Los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, indica el artículo 17 de la LOPD, se establecerán por vía reglamentaria; debemos hacer notar que permanecerán en vigor los procedimientos para el ejercicio de los derechos de acceso, rectificación y cancelación contemplados en el Reglamento que continua vigente[104].

Este procedimiento es de gran importancia, ya que establece, en la práctica, la efectividad de la Ley y el verdadero respeto –que no sólo reconocimiento– a los derechos en ella recogidos.

Ahora bien, es posible que la rectificación o, en su caso, la cancelación, no sea procedente y el responsable del fichero no esté, por tanto, obligado a realizarla; en este caso pondrá en conocimiento del afectado, en el mismo plazo de diez días, la no procedencia de la rectificación o la cancelación solicitada argumentando los motivos por los que no la realiza[105].

Si pasados los diez días, el afectado no recibe respuesta alguna a su solicitud de rectificación o de cancelación, a efectos de interponer la reclamación que corresponda, se entenderá que la solicitud ha sido desestimada.

En el caso del ejercicio de los derechos de rectificación y cancelación la Instrucción 1/1998 también destaca algunas características vía interpretativa que debemos señalar:

1. La solicitud de rectificación que haga el afectado deberá señalar el dato que se considera erróneo y la corrección que se debe realizar, así como acompañar la documentación que lo justifique.

2. Si el responsable del fichero hubiera cedido a un tercero los datos que hayan sido rectificados o cancelados se le deberá comunicar que se ha efectuado la rectificación o cancelación y en qué ha consistido para que él (el tercero cesionario de los datos), actúe en consecuencia.

3. Indica el apartado cuarto de la norma tercera de la Instrucción que estamos comentando que *en la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda,* cuestión a tener en cuenta y que creemos no necesita más comentario.

---

[103] El artículo 16 de la LOPD indica, en su tercer apartado, que "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

[104] Artículos 12 y ss. del Real Decreto 1332/1994.

[105] "En el supuesto de que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente y dentro del plazo señalado en el apartado anterior, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992", indica el apartado tercero, del artículo 15 del Reglamento.

4. Por último, señalar que la solicitud de rectificación o cancelación no resulta de obligado cumplimiento por el responsable del fichero, sino que solamente debe atender la petición pero no está obligado a llevar a cabo la rectificación o la cancelación cuando no sean procedentes.

Conviene reseñar que la normativa señala unos requisitos generales para el ejercicio de los derechos de acceso, rectificación y cancelación [106] entre los que destaca su carácter de personalísimos, pudiendo solamente ser ejercidos por el afectado y ante el responsable del fichero; no es válido, por tanto, el ejercicio de los derechos mediante representante a excepción, cuestión lógica, de aquellas personas que se encuentren en situación de incapacidad jurídica o sean menores de edad, que les imposibilita el ejercicio personal de los derechos y que podrán realizarlo a través de su representante que deberá acreditar ante el titular del fichero su representación.

Llama extraordinariamente la atención que la Instrucción 1/1998, también con carácter general para los derechos de acceso, rectificación y cancelación, indica que todas las personas de la organización del responsable del fichero que tengan acceso a datos de carácter personal [107] deben estar preparadas para poder informar al afectado del procedimiento a seguir para el ejercicio de sus derechos, lo que implica que el responsable del fichero debe tomar las medidas oportunas para garantizarlo.

Añadir que, respecto a los requisitos generales de los tres derechos que nos ocupan, indican, tanto la Ley, como el Reglamento y la Instrucción 1/1998, características operativas que en algunos casos se repiten hasta la saciedad, no presentando ningún aspecto de aclaración, sino que incluso dejan pensar que fueron incluidas de relleno para dar más consistencia o, apariencia al texto; no obstante, sí conviene citar que:

– Los derechos de acceso, rectificación y cancelación son derechos independientes, en el sentido de que no se puede exigir el ejercicio previo de uno de ellos para ejercer otro cualquiera.

– Se deberán ejercer mediante solicitud dirigida al responsable del fichero conteniendo la identificación del afectado [108], la petición que solicita, el domicilio a efectos de notificaciones y los documentos acreditativos que, en su caso, sean necesarios para apoyar la petición que formula.

e. El derecho de oposición

Como ya hemos indicado, la LOPD introduce un nuevo derecho, el derecho de oposición, a raíz de la transposición de la Directiva. Este derecho carece de desarrollo reglamentario, y se encuentra recogido dentro del título dedicado a los principios, concretamente en el artículo 6 destinado al consentimiento, que dice así:

> *4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.*

No obstante hay que tener en cuenta que este derecho, de un lado, como deciamos, no tiene desarrollo reglamentario que especifique su ejercicio, y de otro, la AEPD está interpretando que su ejercicio debe ser conforme con el del derecho de acceso.

---

[106] Además, la LOPD ha añadido el derecho de oposición, pero dicho derecho, por un lado, no se encuentra claramente definido (no hay más que llamar la atención, por ejemplo, sobre su ubicación en el artículo 6.4 dentro del principio del consentimiento) y tampoco está desarrollado reglamentariamente, por lo que no es posible establecer un procedimiento para un derecho sólo enumerado.

[107] Expresión que tiene un contenido muy amplio pues acceso a datos de carácter personal en un sistema automatizado pueden tener múltiples personas, desde los operadores del sistema, programadores, analistas y cualquier otro personal informático; no parece operativo que el afectado pueda dirigirse a cualquiera de estas personas y haya que estructurar una estrategia para poder cumplir con lo indicado en la Instrucción, con la consiguiente inseguridad que para el propio afectado podría esto llevar consigo.

[108] Identificación que la Instrucción 1/1998 centra como válida con la "fotocopia del documento nacional de identidad del afectado", aunque, bien es cierto que podrá ser sustituida siempre "que se acredite la identidad por cualquier otro medio válido en derecho" (segundo párrafo, del apartado tercero, de la norma segunda).

A continuación se presenta una tabla que posibilita la rápida comprensión de los derechos analizados.

TABLA I: DERECHOS DEL INTERESADO

Derecho de impugnación de valoraciones	El derecho de impugnación de valoraciones consiste en: • la facultad del interesado, • de no verse sometido a una decisión con efectos jurídicos, • que le afecte de manera significativa, • efectuada sobre la base de un tratamiento de datos, • destinado a evaluar determinados aspectos de su personalidad.
Derecho de acceso al RGPD	Mediante el ejercicio de este derecho: • cualquier persona podrá recabar información, • ante el Registro General de Protección de Datos (RGPD), • sobre: – la existencia de tratamientos de datos, – o sus finalidades, y – la identidad del responsable del tratamiento • de forma gratuita.
Derecho de acceso	Consiste en la facultad del interesado para: • solicitar, y • obtener información sobre: – sus datos sometidos a tratamiento, – el origen de los mismos, y – las comunicaciones realizadas o que se prevean realizar • de forma gratuita Ejercitándose a intervalos no inferiores a 12 meses, salvo que se acredite un interés legítimo.
Derechos de rectificación y cancelación	Supone la facultad del interesado de: • instar al responsable del fichero a: – rectificar o cancelar, – los datos cuyo tratamiento no se ajuste a la Ley y, en particular, – resulten inexactos o incompletos • en el plazo de diez días.
Derecho de oposición	Consiste en la facultad del interesado para: • oponerse al tratamiento de sus datos, • cuando no sea necesario su consentimiento para el tratamiento, • existan motivos fundados y legítimos para ello, y • una ley no disponga lo contrario.
Características de los derechos	Los derechos de acceso, rectificación y cancelación se caracterizan por ser: • personalísimos, • si bien cabe la actuación del representante legal cuando el interesado se encuentre en situación de: – incapacidad, o – minoría de edad – o que le imposibilite para el ejercicio personal de los mismos • son derechos independientes.
Ejercicio	Los derechos conferidos al interesado: • serán ejercidos ante el responsable del fichero, • mediante solicitud dirigida al mismo con el contenido legalmente determinado, • el ejercicio de uno no es requisito previo para el ejercicio de otro derecho.

7. OBLIGACIONES DEL RESPONSABLE DEL FICHERO

En general, podríamos decir que las obligaciones del responsable del fichero se centran en tomar todas las medidas necesarias orientadas a impedir el abuso o mal empleo de la información, así como hacer un tratamiento de los datos legal y leal; pero no terminan ahí las obligaciones ya que se completan, en ambas direcciones, de forma que el afectado pueda tener conocimiento exacto y real de la situación de sus datos en el fichero, al tiempo que se le facilite el ejercicio de sus derechos.

Así, destacando alguna de las obligaciones más significativas del titular del fichero, diremos que toda persona [109] que mantenga un archivo con datos de carácter personal, está obligada a:

a. Inscribirlo en el Registro General de Protección de Datos

Toda institución, pública o privada, que posea un fichero de datos de carácter personal, tiene la obligación de comunicarlo a la Agencia Española de Protección de Datos que, tras el análisis de su contenido y si cumple con todos los requisitos exigidos por la propia LOPD y por el Reglamento, lo inscribirá en el Registro General de Protección de Datos. También deberán notificarse a la Agencia los cambios que se produzcan *en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.*

No obstante, este análisis no implica un control a priori del cumplimiento de la LOPD ni tampoco supone que el fichero cumpla con estos requisitos en el sentido de que el tratamiento sea legal. Es solamente un trámite administrativo que permite al responsable del fichero o tratamiento cumplir con una de las obligaciones que le impone la normativa sobre protección de datos, si bien el Registro General de Protección de Datos comprueba que la inscripción efectuada cumple con los requisitos exigidos para dicha notificación.

Para realizar estas comunicaciones, la propia Agencia Española de Protección de Datos ha elaborado unos impresos o formularios [110], que facilitan al titular del fichero exponer los requisitos que son exigidos por la Ley y por el Reglamento, entre los que se encuentran la identificación del responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.

b. Tratamiento legal y leal

En este apartado debemos recordar los tres momentos en los que hemos indicado que se configura el tratamiento de datos: 1.- Cuando se recaba el dato. 2.- Cuando se procede al tratamiento. 3.- Cuando el dato es utilizado o cedido; el tratamiento legal y leal debe realizarse en todas las fases, respetando los derechos del afectado y ciñendo el tratamiento a los principios establecidos en la norma.

La inscripción del fichero es solamente la primera obligación pero, al ser "vivo" el tratamiento de los datos (altas, bajas, modificaciones), su utilización y, en su caso, cesión, exigen se haga en forma legal y leal.

El tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención.

---

[109] Tanto física como jurídica, con o sin ánimo de lucro. Solamente no se encuentran bajo el ámbito de aplicación de la Ley, de acuerdo con lo especificado en el apartado tercero del artículo 2, "a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia."

[110] Resolución de 30 de mayo de 2000, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos, publicada en el Boletín Oficial del Estado núm. 153, de 27 de junio. Disponibles en www.agpd.es.

El principio de la lealtad –tanto al recabar los datos, con un conocimiento consciente e informado, como en el tratamiento y en la utilización o cesión posterior–, que tantas veces es discutido y malinterpretado y que no puede servir para encubrir fines diferentes a los que realmente pretende proteger, puede ser, y en muchas ocasiones lo es, punto controvertido en el estudio del tratamiento de datos de carácter personal.

c. Facilitar el ejercicio de los derechos

El titular del fichero tiene la obligación de facilitar, con diligencia, el ejercicio de los derechos al afectado de forma que sea una ayuda que permita la máxima transparencia, y la lealtad en el tratamiento de la que ya hemos hablado; hasta tal punto esto es así que, como hemos dicho, la Instrucción 1/1998 indica que el responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Los plazos en los que se debe hacer efectivo el derecho de rectificación o el de cancelación ejercido por el afectado (diez días[111]), muestran con claridad el interés del legislador en que el titular del dato se encuentre con la atención precisa y rápida por parte del responsable del fichero.

Incluso la obligación de facilitar el ejercicio de los derechos al ciudadano, se lleva al extremo de que la Instrucción 1/1998, obliga al responsable del fichero a solicitar al afectado la subsanación de los defectos que pueda tener su solicitud cuando ésta no reúna los requisitos que exige la norma.

d. Deber de secreto

El responsable del fichero, indica el artículo 10 de la LOPD, y quienes intervengan en cualquier fase del tratatamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Ello implica que, en la práctica, las personas que deban operar sobre los ficheros tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y para poder prevenir el mal uso de los datos.

Es natural esta exigencia si se tiene en cuenta el carácter que el legislador quiere imprimir a los datos de carácter personal cuando son susceptibles de tratamiento, llevando las consecuencias hasta los extremos que se consideren necesarios para garantizar el respeto a la intimidad y, como reza el artículo 18.4 de la Constitución, "el honor personal y familiar".

e. Medidas de seguridad

La seguridad debe ser extremada al máximo para impedir el acceso a los ficheros, en particular, y a los datos en general, a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos; pero la seguridad debe ser también tenida en cuenta para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado.

A la seguridad dedica la LOPD, el artículo 9, indicando que:

> *"El responsable del fichero y, en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado".*

[111] *Estos diez días han de entenderse y computarse, en el caso de los ficheros de titularidad privada, como días naturales, según la interpretación establecida por el Director de la Agencia Española de Protección de Datos con base en lo dispuesto en el apartado 2 del artículo 5 del Código Civil que dispone que "en el cómputo civil de los plazos no se excluyen los días inhábiles".*

artículo que ha sido desarrollado mediante el Real Decreto 994/1999, de 11 de junio, ya citado, que establece unas obligaciones para el titular del fichero, orientadas a la adopción de medidas de índole técnica y organizativas para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos.

Este Real Decreto por el que se aprueba el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal, contempla tres niveles de medidas de seguridad -nivel básico, nivel medio y nivel alto- que se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. Existe también un tipo de ficheros, los que permiten obtener una evaluación de la personalidad del individuo, que tienen que cumplir, además de las medidas de nivel básico, algunas de las de nivel medio, en concreto, las contenidas en los artículos 17 a 20 del Reglamento, por lo que puede hablarse, aunque no en términos estrictos normativamente hablando, de un "nivel intermedio".

e.1. Medidas de seguridad de nivel básico

El nivel básico se aplicará a todos los ficheros que contengan datos de carácter personal y comprende:

a) La creación por el responsable del fichero de un documento de seguridad de obligado cumplimiento para el personal que tenga acceso a los datos y a los sistemas de información y que contendrá las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, la estructura de los ficheros con datos de carácter personal, el procedimiento de notificación, gestión y respuesta de las incidencias, entendiendo por incidencias, cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos y, por último, los procedimientos de realización de copias de respaldo y de recuperación de los datos,

b) La adopción por el responsable del fichero de las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento,

c) La creación de un registro de incidencias en el sentido ya expuesto como tales,

d) La creación de una relación actualizada de usuarios (entendiendo por tales -por usuarios- los sujetos o procesos autorizados para acceder a los datos o recursos), que tengan acceso al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso,

e) El establecimiento de un mecanismo de control de acceso y

f) El establecimiento de un mecanismo de control de soportes.

e.2. Medidas de seguridad de nivel medio

El nivel medio se aplicará a los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito; estos ficheros que son clasificados como de "nivel medio", deberán reunir, además de las medidas de nivel básico que ya hemos referido, las siguientes referentes a que el documento de seguridad deberá contemplar todas las características citadas para los ficheros de nivel básico y además contendrá la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Destacaremos para los ficheros que deben cumplir las medidas de nivel medio que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa que verifique el cumplimiento del propio Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

Completa las exigencias para este tipo de ficheros el establecimiento de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema y la verificación de que está autorizado, limitándose la posibilidad de intentar reiteradamente el acceso no autorizado, junto con otras limitaciones, en este caso de acceso físico a los locales donde se encuentren ubicados los sistemas de información, permitiéndolo solamente a aquellas personas autorizadas.

Por último, se establecen normas para la gestión de soportes, procedimientos de recuperación de datos y pruebas con datos reales que no estarán permitidas salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

e.3. Medidas de seguridad de nivel alto

El nivel alto se aplicará a los ficheros que contengan datos de los que denomina la LOPD especialmente protegidos [112], así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

Estos ficheros deberán reunir, además de las medidas establecidas para los de nivel básico y las establecidas para los de nivel medio, otras medidas complementarias relativas a la distribución de soportes, al registro de accesos, a las copias de respaldo y recuperación y, en caso de que se realice transmisión de datos a través de redes de telecomunicaciones, se exige el cifrado de los mismos.

Vemos, por tanto, que no se trata solamente de cumplir una normativa sobre protección de datos en la forma que estamos indicando, sino también de establecer unas medidas de seguridad mínimas, exigibles a todos los titulares de ficheros, que garanticen la propia seguridad e integridad de la información cuando se trata de utilización de datos de carácter personal.

Es el titular del fichero quien debe adoptar, y, por tanto, será responsable de ello, de acuerdo con lo que especifica el apartado primero del artículo 9 de la LOPD, *las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

Dado el enorme interés y consecuencias prácticas que la adopción e implementación de las medidas de seguridad tienen para la empresa, hemos considerado, en aras a proporcionar la mayor utilidad para el gestor, necesario y sumamente conveniente exponer las medidas de seguridad en una tabla analítica.

[112] *A los que ya nos hemos referido anteriormente y que son los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y a la comisión de infracciones penales o administrativas.*

TABLA II. MEDIDAS DE SEGURIDAD

Documento de Seguridad (arts. 8 y 15)	Existencia de una normativa de seguridad descrita en un documento de obligado cumplimiento para todo el personal con acceso a los ficheros. Contenido del Documento de Seguridad: • Ámbito de aplicación con especificación detallada de los recursos protegidos • Medidas, normas, procedimientos y estándares • Funciones y obligaciones del personal • Estructura de los ficheros de datos y los sistemas de información que los tratan • Procedimientos de notificación, gestión y respuesta ante las incidencias • Procedimiento de actualización de los últimos cambios producidos en la aplicación o en la organización • Adecuación a las últimas disposiciones vigentes en materia de seguridad de datos • Identificación del responsable de seguridad • Controles periódicos para verificar lo dispuesto en el documento de seguridad • Medidas a adoptar para el desechado o reutilización de soportes
Funciones y obligaciones del personal (art. 9)	Las funciones y obligaciones de cada una de las personas con acceso a: • Los datos de carácter personal • Los sistemas de información estarán claramente definidas y documentadas El responsable del fichero adoptará las medidas necesarias para que el personal conozca: • Las normas de seguridad que afectan al desarrollo de sus funciones • Las consecuencias en que pudiera incurrir en caso de incumplimiento
Responsable de Seguridad (art. 16)	Designación de uno varios responsables de seguridad por el responsable del fichero para coordinar y controlar las medidas definidas en el Documento de Seguridad
Registro de incidencias (arts. 10 y 21)	Constará: • El tipo de incidencia • El momento en que se ha producido • Persona que lo notifica • A quién se lo comunica • Los efectos derivados de la misma Procedimientos realizados de recuperación de datos, persona que ejecutó el proceso, datos restaurados y los datos que han sido necesarios grabar manualmente. Necesidad de autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de datos.
Identificación y autenticación (arts. 11 y 18)	Existencia de una relación actualizada de usuarios con acceso autorizado al sistema de información y procedimientos de identificación y autenticación para dicho acceso. Procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad de las contraseñas empleadas como mecanismo de autenticación. Periodicidad del cambio de contraseñas y almacenamiento de forma ininteligible mientras estén vigentes. Mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema de información y la verificación de que está autorizado. Limitación de la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.

TABLA II. MEDIDAS DE SEGURIDAD (Continuación)

Control de acceso (art. 12)	Los usuarios únicamente tendrán acceso a los datos o recursos que precisen para el desarrollo de sus funciones. El responsable del fichero establecerá los mecanismos para evitar el acceso a datos o recursos con derechos distintos a los autorizados. La relación de usuarios con acceso al sistema de información contendrá el acceso autorizado para cada uno de ellos. Exclusivamente el personal autorizado en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado conforme a los criterios establecidos por el responsable del fichero.
Control de acceso físico (art. 19)	Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información.
Gestión de soportes (arts. 13 y 20)	Los soportes informáticos que contengan datos deberán: • Permitir identificar el tipo de información que contienen • Ser inventariados • Almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad La salida fuera de los locales en los que esté ubicado el fichero únicamente podrá ser autorizada por el responsable del fichero. El sistema de registro de entrada deberá permitir, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de recepción que deberá estar debidamente autorizada. El sistema de registro de salida permitirá, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. En caso de desecho o reutilización de soportes se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario. En caso de operaciones de mantenimiento fuera de los locales en que se encuentren ubicados los ficheros, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.
Copias de respaldo y recuperación (arts. 14 y 25)	El responsable del fichero verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación. Los procedimientos establecidos deberán garantizar la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se haya producido ninguna actualización de los datos. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de datos en un lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad exigidas.
Auditoría (art. 17)	Externa o interna de los sistemas de información e instalaciones de tratamiento, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad, al menos, cada dos años.

TABLA II. MEDIDAS DE SEGURIDAD (Continuación)

Auditoría (art. 17)	El informe de auditoría dictaminará sobre la adecuación de las medidas y controles al Reglamento, identificando las deficiencias y proponiendo las medidas correctoras o complementarias necesarias. Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. Los informes de auditoría serán analizados por el responsable de seguridad, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos.
Pruebas con datos reales (art. 22)	Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
Registro de accesos (art. 24)	Como mínimo, se guardará de cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso ha sido autorizado, se guardará la información que permita identificar el registro accedido. Los mecanismos que permiten el registro de los datos anteriores estarán bajo el control del responsable de seguridad sin que se deba permitir su desactivación. Los datos registrados se conservarán durante un período mínimo de dos años. El responsable de seguridad revisará periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.
Distribución de soportes (art. 23)	Se realizará cifrando los datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.
Telecomunicaciones (art. 26)	La transmisión de datos a través de redes de telecomunicaciones se hará mediante su cifrado o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

A continuación recogemos un checklist de comprobación de las medidas de seguridad, cuya utilidad consideramos máxima pues sirve, de un lado, para comprobar la implantación de las mismas en la entidad y, de otro, para adoptarlas, en caso de que aún no se haya hecho. Con el fin de proporcionar una herramienta lo más completa posible, hemos incluido el checklist que se utilizaría para un fichero de nivel alto, pues, como las obligaciones son acumulativas, se tiene asimismo que cumplir las medidas de nivel básico y medio. Para diferenciar el nivel al que pertenece cada medida se ha añadido entre paréntesis una indicación: B (básico), M (medio) y A (alto).

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Tipos de ficheros (B)	
Estructura de los ficheros (B)	
Tipos de programas (B)	
Tipos de soportes (B)	
Sistema de registro de entrada de soportes informáticos: (M) Tipo de soporte Fecha y hora Emisor Número de soportes Tipo de información contenida Forma de envío Responsable autorizado recepción	
Sistema de registro de salida de soportes informáticos: (M) Tipo de soporte Fecha y hora Destinatario Número de soportes Tipo de información contenida Forma de envío Responsable autorizado recepción	
Soportes reutilizados (M) Medidas de control Imposibilidad recuperar información	
Soportes desechados (M) Medidas de control Imposibilidad recuperar información	
Distribución de soportes con información (A) Garantía inteligibilidad Garantía de no manipulación	
Tipos de equipos (B)	
Sistemas de información (B)	
Transmisión de datos por redes de telecomunicaciones (A) Garantía inteligibilidad Garantía de no manipulación	
Procedimientos de identificación (B)	
Procedimientos de autenticación (B)	

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO (continuación)

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Si contraseñas (B) Asignación Distribución Almacenamiento Garantía de confidencialidad Garantía de integridad Periodicidad en el cambio Almacenamiento ininteligible	
Relación actualizada usuarios con acceso autorizado (B) Sujetos Procesos	
Acceso autorizado (B) Según usuario Según funciones	
Criterios de (B) Concesión Alteración Anulación Del acceso autorizado	
Quién puede Conceder Alterar Anular el acceso autorizado	
Verificación autorización acceso (M) Registro de accesos (A) Identificación usuario Fecha y hora Fichero accedido Tipo de acceso Autorización de acceso Identificación registro accedido Denegación de acceso Conservación 2 años datos registrados	
Mecanismos registros de accesos (A)	
Revisión información registros de accesos (A)	
Informe mensual revisiones realizadas (A)	
Informe mensual problemas detectados (A)	
Personal autorizado en locales de ubicación del sistema (M) Control de acceso físico	
Ejecución tratamiento fuera de locales (B) Autorización escrita responsable fichero	

TABLA III: CHECKLIST DE MEDIDAS DE SEGURIDAD DE NIVEL ALTO (continuación)

CONCEPTO	CUMPLIMIENTO PRÁCTICO
Funciones del personal (B)	
Documentación funciones del personal (B)	
Responsable de seguridad (M) Coordinación/control medidas Conclusiones informe auditoría	
Procedimiento notificación incidencias (B)	
Procedimiento gestión incidencias (B)	
Procedimiento respuesta incidencias (B)	
Registro de incidencias (B) Tipo de incidencia Momento de su producción Persona que la notifica Persona a la que se comunica Efectos de la incidencia Procedimientos recuperación datos (M) Persona ejecuta proceso Datos restaurados Datos grabados manualmente en la recuperación	
Auditoría externa o interna cada dos años mínimo (M)	
Informe de auditoría (M) Adecuación medidas Adecuación controles Identificación deficiencias Propuesta medidas correctoras Documentación conclusiones Datos Hechos Observaciones	
Medidas correctoras adoptadas según informe de auditoría (M)	
Copias de respaldo (B) Periodicidad semanal mínima (salvo no alteración) Conservación en lugar distinto al de ubicación equipos (A)	
Copias de recuperación (B) Procedimientos Conservación copia en lugar distinto al de ubicación equipos (A) Aplicación Garantía reconstrucción íntegra	
Autorización por escrito de procedimientos recuperación de datos (M)	
Actualización del documento (B)	
Revisión documento por cambios relevantes en sistema de información (B)	
Adecuación del documento (B)	

8. PROCEDIMIENTOS

El ciclo del tratamiento de los datos y de su protección correspondiente en defensa del derecho fundamental que hemos expuesto, se concluye con los denominados procedimientos.

Aunque haya que respetar por la empresa titular del fichero los principios de la protección de datos contemplados en la norma y que hemos expuesto; aunque la empresa ponga todos los medios para que el interesado pueda ejercer sus derechos y sea atendido en los plazos indicados, aunque se den todas estas cosas, deben existir unos procedimientos mediante los cuales el ciudadano pueda verse tutelado en el caso de que considere que no se está produciendo un tratamiento de datos legal.

A estos procedimientos dedicamos nuestra atención de una forma específica por la importancia que tienen para completar un tratamiento de datos en nuestra entidad que sea, como ya hemos indicado varias veces, legal y leal.

a. Procedimiento de inscripción de ficheros

Una empresa puede tomar la decisión de crear un fichero de datos de carácter personal cuando lo considere conveniente para sus intereses y desarrollo de su objeto social.

Ahora bien, una vez tomada esta decisión hay que proceder a inscribir ese fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Los artículos 25 a 30 de la LOPD, regulan –respecto a los ficheros de titularidad privada–, la creación, notificándolo previamente a la Agencia Española de Protección de Datos (art. 26.1), remitiendo a posterior desarrollo reglamentario [113] respecto al contenido de esta notificación que, no obstante, se exige que necesariamente figure (art. 26.2)

> *"El responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar".*

Tras esta comunicación, y si se ajusta y cumple con todos los requisitos, el fichero se inscribirá en el Registro General de Protección de Datos (art. 26.4).

En el Real Decreto 1332/1994 [114] figura el procedimiento para la notificación e inscripción de ficheros y a ese lugar nos remitimos; no obstante, conviene decir que la Agencia Española de Protección de Datos ha elaborado unos impresos para la inscripción, modificación y supresión o baja de ficheros y recomienda, además, que la inscripción se realice a través de Internet [113].

b. Procedimiento de acceso

El procedimiento de acceso, que la LOPD indica, será establecido reglamentariamente [116], se encuentra regulado en el Reglamento (artículos 12 a 16) y "aclarado" [117] en la Instrucción 1/1998, exponiendo tanto las características y requisitos que debe contener el ejercicio de los derechos para que puedan hacerse efectivos, como el contenido de la información que el titular del fichero debe proporcionar al afectado cuando éste la solicite.

---

[113] Desarrollado mediante el Real Decreto 1332/1994, citado.

[114] En el capítulo III, artículos 6 a 8, del Real Decreto 1332/1994, figura el procedimiento de notificación de los ficheros de titularidad privada y el de inscripción de los mismos; repetir en este lugar esos artículos no nos ha parecido adecuado.

[115] Resolución de 30 de mayo de 2000, ya citada anteriormente.

[116] Primer apartado del artículo 17 de la LOPD.

[117] Según expresión literal de la introducción de la Instrucción 1/1998 al indicar que "esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación", aunque nosotros creemos que lo que realmente hace es mostrar la interpretación que la Agencia Española de Protección de Datos da a la LOPD y al Reglamento, respecto al ejercicio por el afectado de los citados derechos.

Cabe destacar que la Instrucción 1/1998 incluyó alguna novedad significativa tanto en la solicitud, por el afectado, del derecho, como en la respuesta que le debe dar el titular del fichero. Señalamos, por ejemplo, la obligación, en ambos casos, del afectado y del titular o responsable del fichero, de acreditar el envío y la recepción de la solicitud en el caso del afectado[118], como el envío y la recepción de la respuesta en el caso del responsable del fichero.

La forma de ejercer los derechos, en la práctica, mediante solicitud dirigida al responsable del fichero, queda clara tanto en la redacción que da el Reglamento como en la, casi idéntica, que da la Instrucción 1/1998 y que se plasma en el apartado tercero, de la norma primera, de la Instrucción, que indica:

> *El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:*
>
> *Nombre, apellidos del interesado y fotocopia del documento nacional de identidad del interesado y en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.*
>
> *Petición en que se concreta la solicitud.*
>
> *Domicilio a efectos de notificaciones, fecha y firma del solicitante.*
>
> *Documentos acreditativos de la petición que formula, en su caso.*

Indicando también que, al ejercitar el derecho de acceso, el afectado podrá optar por:

> *Uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:*
>
> *a) Visualización en pantalla*
>
> *b) Escrito, copia o fotocopia remitida por correo*
>
> *c) Telecopia*
>
> *d) Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero, ofrecido por el responsable del mismo*

El responsable del fichero debe contestar a la indicada solicitud tanto si en el fichero figuran datos del afectado que ha realizado la solicitud, como si no figura ningún dato sobre dicha persona.

c. Procedimientos de reclamación en vía administrativa

Si el ciudadano considera que sus datos no son tratados correctamente y cree que debe ser tutelado en sus derechos, puede acudir al órgano de control de cumplimiento de la Ley (la Agencia Española de Protección de Datos), a solicitar que se atiendan sus reclamaciones encaminadas a hacer efectivo y real el cumplimiento de la norma por el titular del fichero.

De entre estos procedimientos que la Ley contempla en vía administrativa señalamos por su interés el procedimiento de tutela de derechos y el procedimiento sancionador.

[118] *Último párrafo, del apartado tercero, de la norma primera de la Instrucción 1/1998.*

c.1. Procedimiento de tutela de derechos

El ejercicio de los derechos que otorga a los ciudadanos la Ley se lleva a cabo mediante un procedimiento de tutela, que podemos orientar en la línea de lo que se ha dado en llamar el "habeas data", como instrumento que permite facilitar un camino mediante el que el afectado puede ejercer la defensa de los derechos que se pretende proteger[119].

En el caso español, el Real Decreto 1332/1994, de 20 de junio, citado, regula determinados aspectos, *en su mayoría de orden procedimental, referentes al ejercicio de los derechos de acceso, rectificación y cancelación, a la forma de reclamar ante la Agencia Española de Protección de Datos por actuaciones contrarias a la Ley, a la notificación e inscripción de los ficheros automatizados de datos y al procedimiento para la determinación de las infracciones y la imposición de las sanciones.*

El procedimiento de tutela de derechos se encuentra regulado en el artículo 17 del Reglamento, indicando que se debe iniciar siempre a instancia del afectado, mediante escrito de reclamación ante la Agencia Española de Protección de Datos; en el referido escrito se debe indicar con claridad el contenido de su reclamación y los preceptos de la Ley que se consideren vulnerados[120].

Recibida la reclamación se da traslado de la misma al responsable del fichero para que formule las alegaciones que considere convenientes y, tras audiencia al afectado y de nuevo al responsable del fichero, el Director de la Agencia Española de Protección de Datos resolverá dando traslado a los interesados de la resolución, cabiendo recurso contencioso-administrativo contra la misma.

c.2. Procedimiento sancionador

El procedimiento sancionador se encuentra regulado en los artículos 18 y 19 del Reglamento; se inicia siempre de oficio por la Agencia Española de Protección de Datos, bien haya tenido conocimiento por denuncia del afectado o de un tercero, o por otros motivos o actos, como puede ser el ejercicio de la actividad inspectora.

Algo más complejo en su desarrollo que el procedimiento de tutela de derechos, el sancionador se inicia mediante acuerdo del Director de la Agencia Española de Protección de Datos, en el que se designará instructor con indicación de la posibilidad de recusación y se identificará al presunto responsable, o responsables, concretando los hechos y la infracción que, supuestamente, ha cometido, así como la sanción o sanciones que se pueden imponer y las medidas cautelares a adoptar en su caso.

Una vez se notifique al presunto responsable la incoación del expediente, ofreciéndole la posibilidad de efectuar alegaciones y de emplear los medios de prueba de que se quiera valer, se ordenará por el instructor la práctica de las mismas y volverá a poner de manifiesto el expediente al presunto responsable para que, a la vista del resultado de las pruebas, pueda alegar nuevamente, incluso aportando documentos, lo que considere de interés.

Por último, el instructor formulará una propuesta de resolución motivada que notificará al presunto responsable para que, en un nuevo plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno.

Termina el procedimiento con la notificación al responsable de la resolución que determinará con precisión los hechos imputados, la infracción cometida, el responsable de la misma y la sanción impuesta, o la declaración de no existencia de responsabilidad, expresando también el derecho de interponer contra la misma el correspondiente recurso contencioso-administrativo.

---

[119] *Ya hemos indicado en algún otro comentario a la Ley española –exactamente al proyecto de ley español, pues tal era en aquel entonces– que el procedimiento debe ser tal que su ejercicio no levante sospechas y el cauce procedimental esté suficientemente garantizado, ya que el órgano que se cree para ello, en su caso, si no goza de esa independencia, puede llegar a ser un nuevo santuario burocrático, donde se reciba la esperanza de protección para devolver desengaños traumáticos. Seguimos opinando de la misma forma sobre este tema y lo seguiremos exponiendo. Cfr. Davara, M.A. "Intimidad, informática y seguridad jurídica en España". Boletín de la Fundación para el Desarrollo Social de las Comunicaciones (128) FUNDESCO. Madrid. abril 1992. pg. 14.*

[120] *Nosotros entendemos que lo que debe figurar con claridad es el contenido de su reclamación porque no creemos que se debe dejar de atender una petición de tutela de derechos de un ciudadano porque no vengan expresados "con claridad" los preceptos de la Ley que se consideren vulnerados.*

La calificación de los hechos y, consecuentemente, la sanción a imponer, está resultando tema controvertido pues la Agencia Española de Protección de Datos realiza una interpretación *"sui generis"* de la Ley que ha concluido con la imposición de múltiples multas de elevadas cantidades. La lentitud de los órganos jurisdiccionales, en particular, la Audiencia Nacional, está resultando gravemente dañosa y haciendo, en la práctica, que el órgano de control del cumplimiento de la Ley se haya convertido en un órgano atemorizante, más que en un órgano de apoyo interpretativo y de tutela de derechos.

9. CÓDIGOS TIPO

La LOPD prevé que tanto los responsables de ficheros de titularidad pública como privada puedan elaborar códigos tipo, éticos, deontológicos o de conducta, con el fin de adaptar las disposiciones y la interpretación de la Ley a un sector particular. Esta previsión de la LOPD trae causa de lo dispuesto en el artículo 27 de la Directiva 95/46/CE, en el que se insta a los Estados miembros y a la Comisión Europea a alentar la elaboración de códigos de conducta que permitan una mejor aplicación de las disposiciones nacionales sobre protección de datos teniendo en consideración las particularidades de cada sector.

Estos códigos tipo deben ser inscritos en el Registro General de Protección de Datos, para lo cual es necesario que cumplan con unos requisitos de forma y de fondo, de manera que es necesario que el código aporte un valor añadido al mero cumplimiento de las disposiciones de la LOPD.

10. INFRACCIONES Y SANCIONES

El Título VII de la LOPD, bajo el epígrafe de "infracciones y sanciones", regula (arts. 43 a 49), un régimen sancionador al que estarán sometidos los responsables de los ficheros y en el que se califican las infracciones como leves, graves y muy graves (art. 44), estableciéndose multas que van desde los seiscientos un euros con un céntimo (cien mil pesetas), a los seiscientos un mil doce euros con diez céntimos (cien millones de pesetas), graduándose la cuantía atendiendo a (art. 45.4):

> *"La naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora".*

Las infracciones prescribirán a los tres años las muy graves, a los dos las graves y al año las leves, comenzándose a contar el plazo de la prescripción desde el día en que la infracción se haya cometido y, con relación a las sanciones, también se establece un plazo de prescripción siendo de tres años las que hayan sido impuestas como consecuencia de faltas muy graves, de dos años las consecuentes de faltas graves y de un año las que provengan de faltas leves.

Cuando se cometa una infracción calificada como muy grave, de forma que se estén utilizando o cediendo los datos personales atentando gravemente contra los derechos *"de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan",* el Director de la Agencia Española de Protección de Datos, además de ejercer la potestad sancionadora, podrá requerir a los responsables de los ficheros la cesación de esa ilícita utilización o cesión de datos (art. 49), pudiendo, en caso de no ser atendido en su requerimiento, inmovilizar los ficheros.

Precisamente son las sanciones tan elevadas las que a veces nos llevan a pensar si de verdad esta norma es una norma equilibrada y acorde con el derecho que pretende proteger.

Es cierto que se trata de un derecho fundamental pero también es cierto que somos el país del mundo con sanciones económicas más altas; y, además, con mucha diferencia.

Preguntamos, ¿es lógico que un error informático en el que no exista mala fe pueda llevar, por cada caso denunciado, a una sanción de hasta seiscientos mil y pico euros, esto es, de hasta cien millones de pesetas?

No queremos dar respuesta a la pregunta ya que no es éste el objeto de la obra, pero sí queremos llamar la atención a los responsables de las empresas sobre que las multas se están aplicando con rigor y no hay más que leer las anuales memorias de la Agencia Española de Protección de Datos para comprobar que esto es así.

Cuando menos se lo piensa uno se encuentra con una sanción, de elevada cuantía, que hace que nos planteemos muchas preguntas; pero no es el lugar, ni el momento, para seguir con esta argumentación.

Cumplamos con la protección de datos porque es un derecho fundamental de todos y debemos respetar los principios y el ejercicio de los derechos de los interesados que hemos expuesto. Cumplamos con la protección de datos porque es nuestra obligación cumplir con todas las normas y porque ésta, además, se presenta como una garantía de seguridad y de desarrollo de nuestra empresa sin problemas añadidos.

De esta forma, cumpliendo con la protección de datos, además evitaremos fuertes sanciones.

11. TRANSFERENCIA INTERNACIONAL DE DATOS

El desarrollo global del comercio, y más en concreto la plasmación que ha tenido en un fenómeno social como es el comercio electrónico, y la presencia de las multinacionales tanto en Estados Unidos, principalmente, como en la Unión Europea, ha supuesto la necesidad de arbitrar una serie de normas que regulen la transmisión de datos personales entre entidades que pueden encontrarse en cualquier parte del mundo.

Muestra de lo anterior ha sido la publicación de varias Decisiones por parte de la Comisión de las Comunidades Europeas con terceros países para garantizar la protección de los datos y, en concreto, la Decisión sobre el Acuerdo de Puerto Seguro que regula las transferencias internacionales de datos que tengan por destino a entidades norteamericanas que se hayan adherido a dicho sistema.

Además de la anterior, la Comisión Europea ha aprobado Decisiones relativas al nivel de protección de datos adecuado conferido por Hungría[121], Suiza, Canadá, Argentina, Bailía de Guernsey e Isla de Man, lo que supone que puedan llevarse a cabo transferencias de datos desde un Estado miembro de la Unión Europea con destino a alguno de estos países sin mayores dificultades.

Asimismo, la Comisión Europea ha elaborado dos Decisiones relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países, en virtud de las cuales podrán transferirse datos, de un lado, entre un responsable del tratamiento situado en la Unión Europea y un destinatario de los mismos que se encuentre en un tercer Estado y, de otro lado, entre un responsable del fichero establecido en un Estado miembro de la Unión Europea y un encargado del tratamiento establecido en un tercer país, garantizando al titular de los datos una protección mínima y necesaria conforme a lo dispuesto en la normativa comunitaria. Y ello, sin perjuicio de la posibilidad de realizar dichas transferencias mediante otros contratos, siempre y cuando se haya obtenido la autorización previa de la Agencia Española de Protección de Datos.

[121] Actualmente, la Decisión por la que se declaraba a Hungría como un país con nivel adecuado de protección ha perdido su fundamento puesto que recientemente Hungría ha entrado a formar parte de la Unión Europea.

En particular, a la transferencia de datos entre distintos países dedica la LOPD el Título V que, bajo el epígrafe de "Movimiento internacional de datos", contiene los artículos 33 y 34 bajo la teoría general de que no podrán realizarse transferencias temporales ni definitivas con destino a otros países que no proporcionen un nivel de protección equiparable al que presta nuestra Ley y siempre se realizarán con la autorización previa del Director de la Agencia Española de Protección de Datos que deberá asegurarse de que existen las garantías suficientes.

A esta norma general, se establecen algunas excepciones con base en la aplicación de tratados o convenios en los que sea parte España, cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional, cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, cuando se refiera a transferencias dinerarias conforme a su legislación específica, o cuando el interesado haya dado su consentimiento, 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 propio interesado.

Para conocer cómo se deben interpretar estas normas, de acuerdo con la línea doctrinal seguida por la Agencia Española de Protección de Datos, y tener la garantía de que cuando transferimos datos a terceros países lo estamos haciendo sin riesgo de incumplimiento de la norma y, por tanto, sin riesgo a ser sancionados, se debe acudir a la Instrucción 1/2000[122] relativa a la transferencia internacional de datos centrada en las características que, en opinión del Director de la Agencia Española de Protección de Datos, se deben contemplar en el momento en que necesitemos realizar una transferencia de datos a otro país.

La referida Instrucción en su norma segunda indica que

> *La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento.*

Con el estudio y aplicación del resto de la Instrucción, comprobamos que si se cumple con la garantía de los principios de la protección de datos y los derechos de las personas, contemplados en la LOPD, es posible que no se burle la protección en la transferencia internacional realizada a un Estado que forme parte de la Unión Europea, o a un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, pero también sirve el análisis de la Instrucción para conocer cuáles son las posibilidades que ofrece la Ley para transferir datos a otros países en los que no exista ninguna protección.

12. PROTECCIÓN DE DATOS E INTERNET

Vista la importancia que adquiere la protección de datos, como garantía de una correcta actuación por parte de quien trata los datos y del respeto que puede esperar el titular de los mismos, se hace imprescindible recordar que en el tratamiento de datos efectuado a través de Internet u otros medios de comunicación electrónica también tiene que garantizarse la aplicación tanto de la normativa comunitaria en la materia, como de las normas que regulan en nuestro Ordenamiento jurídico la protección de datos igual al que tienen en otros ámbitos.

Es necesario tomar en consideración que en Internet aparecen sujetos específicos, tales como la operadora de telecomunicaciones, el proveedor de acceso a Internet o el proveedor de servicios de Internet, que para el desarrollo de su actividad y la prestación de sus servicios requieren del tratamiento de los datos de los usuarios, y que por tanto, quedan sometidos a la normativa sobre protección de datos general y específica en el sector de las telecomunicaciones (comunicaciones electrónicas).

[122] *Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, publicada en el Boletín Oficial del Estado número 301, de 16 de diciembre.*

Al igual que ocurre en el entorno no electrónico o físico *(off line),* la protección de datos en Internet se convierte en una obligación para quienes tratan datos de los usuarios y en una garantía para estos últimos. Si bien dicha protección habrá de ser el resultado de una combinación entre las disposiciones legales, recordando que no todos los ordenamientos jurídicos tratan la cuestión de la misma forma, y las diferentes soluciones tecnológicas que desde la industria del hardware y software se desarrollen para dar soluciones específicas a esta cuestión. Un claro ejemplo de esto último puede verse, entre otros, en la Plataforma de Preferencias de Privacidad (P3P) que ayudaría a quienes recaban datos a cumplir la normativa, y a los usuarios que los proporcionan a estar mejor informados y poder tomar las decisiones oportunas.

13 RÉGIMEN SANCIONADOR

Sin intención de convertir el régimen sancionador en una de las razones para el cumplimiento de la Ley, ya que debe recordarse una vez más que el tratamiento efectuado por el responsable del fichero debe ser no sólo legal sino también leal lo que supone que no se incurriera en ninguna infracción, sí debe mencionarse que la infracción de alguna de las normas por parte de quien trata datos de carácter personal lleva aparejadas sanciones que van desde los 601,01 euros (100.000 pesetas) hasta los 601.012 euros (cien millones de pesetas), en el caso de ficheros de titularidad privada, y podrá suponer la iniciación de las actuaciones disciplinarias correspondientes cuando se trate de ficheros de los que sea responsable la Administración Pública.

En virtud de lo dispuesto en la ley están sujetos al régimen sancionador tanto el responsable del fichero como el encargado del tratamiento, lo que supone que tengan que responder personalmente por las infracciones en que hubieran incurrido al tratar datos de carácter personal.

Cabe señalar que las infracciones se clasifican en leves, graves y muy graves. Por lo que se refiere a su prescripción, las infracciones muy graves prescriben a los tres años, las graves a los dos años y las leves al año, comenzando a contarse el plazo de prescripción desde el día en que la infracción se hubiera cometido.

Por último, el procedimiento sancionador se encuentra regulado en los artículos 18 y 19 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, subsistente en virtud de la Disposición Transitoria tercera de la LOPD.

anexo I

DIRECCIONES DE INTERNET

Agencia Española de Protección de Datos: http://www.agpd.es

Agencia Estatal de Administración Tributaria: http://www.aeat.es

Agencia de Protección de Datos de la Comunidad de Madrid: http://www.madrid.org/apdcm

Agencia Catalana de Protección de Datos: http://www.adpcat.net

Asociación Iberoamericana de Cámaras de Comercio (AICO): http://www.aico.org

Boletín Oficial del Estado: http://www.boe.es

Cámara de Comercio Internacional (ICC, International Chamber of Commerce): http://www.iccwbo.org

Camerdata: http://www.camerdata.es

Camerfirma: http://www.camerfirma.com

CAMERPYME: http://www.camerpyme.com

Comisión Europea: http://www.europa.eu.int/comm

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: http://www.uncitral.org

Congreso de los Diputados: http://www.congreso.es

Consejo Superior de Cámaras de Comercio, Industria y Navegación de España: http://www.camaras.org

Corte Española de Arbitraje: https://www.camaras.org/publicado/arbitraje/corte_330.html

Davara & Davara Asesores Jurídicos: http://www.davara.com

Eurocámaras (Eurochambres): http://www.eurochambres.net

Ministerio de Industria, Turismo y Comercio: http://www.min.es

Ministerio de Economía y Hacienda: http://www.mineco.es

Ministerio de Justicia: http://www.mju.es

Organización para la Cooperación y el Desarrollo Económico: http://www.ocde.org

Organización Mundial del Comercio: http://www.wto.org

Parlamento Europeo: http://www.eurparl.eu.int

Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información: http://www.setsi.min.es

Senado: http://www.senado.es

Sitios web de las Cámaras de Comercio (por orden alfabético)

Cámara de Comercio de Almería: http://www.camaralmeria.com
Cámara de Comercio de A Coruña: http://www.camaracoruna.com
Cámara de Comercio de Alava: http://www.camaradealava.com
Cámara de Comercio de Albacete: http://www.camaranet.com/albacete
Cámara de Comercio de Alcoy: http://www.camaraalcoy.net
Cámara de Comercio de Alicante: http://www.camara-alc.es
Cámara de Comercio de Andujar: http://www.camaraandujar.com
Cámara de Comercio de Arevalo: http://www.carevalociudad.com/html/camara
Cámara de Comercio de Astorga: http://www.astorga.com/empresa/ccomerci.htm
Cámara de Comercio de Ávila: http://www.camaranet.com/avila
Cámara de Comercio de Avilés: http://www.avilescamara.com
Cámara de Comercio de Ayamonte: http://www.ayamonte.com
Cámara de Comercio de Badajoz: http://www.camarabadajoz.com
Cámara de Comercio de Barcelona: http://www.cambrabcn.es
Cámara de Comercio de Béjar: http://www.camarabejar.com
Cámara de Comercio de Bilbao: http://www.camarabilbao.com
Cámara de Comercio de Briviesca: http://www.cocicyl.es/Camaras/Briviesca/e-informacion.html
Cámara de Comercio de Burgos: http://www.camaraburgos.com
Cámara de Comercio de Cáceres: http://www.camaracaceres.es
Cámara de Comercio de Cádiz: http://www.camaracadiz.com
Cámara de Comercio de Campo de Gibraltar: http://www.camaracordoba.com
Cámara de Comercio de Cantabria: http://www.camaracantabria.com
Cámara de Comercio de Cartagena: http://www.cocin-cartagena.es
Cámara de Comercio de Castellón: http://www.camaracs.es
Cámara de Comercio de Ceuta: http://www.camaraceuta.org
Cámara de Comercio de Ciudad Real: http://www.camaracr.org
Cámara de Comercio de Córdoba: http://www.camaragranada.org
Cámara de Comercio de Cuenca: http://www.camaracuenca.org
Cámara de Comercio de Ferrol: http://www.camaraferrol.org
Cámara de Comercio de Formentera: http://www.cambresbalears.com
Cámara de Comercio de Gijón: http://www.camaragijon.com
Cámara de Comercio de Girona: http://www.cambra.gi
Cámara de Comercio de Granada: http://www.camaragranada.org
Cámara de Comercio de Guadalajara: http://www.camaranet.com/guadalajara
Cámara de Comercio de Guipúzcoa: http://www.camaragipuzkoa.com
Cámara de Comercio de Huelva: http://www.camarahuelva.com
Cámara de Comercio de Huesca: http://www.camarahuesca.com
Cámara de Comercio de Ibiza: http://www.cambresbalears.com
Cámara de Comercio de Jaén: http://www.camarajaen.com
Cámara de Comercio de Jerez de la Frontera: http://www.camaraenaccion.com
Cámara de Comercio de La Rioja: http://www.camararioja.com
Cámara de Comercio de Las Palmas: http://www.camaralaspalmas.com
Cámara de Comercio de León: http://www.camaraleon.com
Cámara de Comercio de Linares: http://www.camaradelinares.org

Cámara de Comercio de Lorca: http://www.camaracomlorca.es
Cámara de Comercio de Lugo: http://www.camaralugo.com
Cámara de Comercio de Lleida: http://www.cambralleida.com
Cámara de Comercio de Madrid: http://www.camaramadrid.es
Cámara de Comercio de Málaga: http://www.camaramalaga.com
Cámara de Comercio de Mallorca: http://www.cambresbalears.com
Cámara de Comercio de Manresa: http://www.cambramanresa.com
Cámara de Comercio de Menorca: http://www.camaramenorca.com
Cámara de Comercio de Miranda: http://www.camaramiranda.com
Cámara de Comercio de Motril: http://www.camaramotril.com
Cámara de Comercio de Murcia: http://www.cocin-murcia.es
Cámara de Comercio de Navarra: http://www.camaranavarra.com
Cámara de Comercio de Ourense: http://www.camaraourense.com
Cámara de Comercio de Oviedo: http://www.camara-ovi.es
Cámara de Comercio de Palamós: http://www.cambrescat.es/palamos/p-01.htm
Cámara de Comercio de Palencia: http://www.cocipa.es
Cámara de Comercio de Pontevedra: http://www.camaranet.com/pontevedra
Cámara de Comercio de Reus: http://www.cambrareus.org
Cámara de Comercio de Sabadell: http://www.cambrasabadell.org
Cámara de Comercio de Salamanca: http://www.camarasalamanca.com
Cámara de Comercio de Sant Feliu: http://www.cambrescat.es/stfeliu/p-01.htm
Cámara de Comercio de Santa Cruz de Tenerife: http://www.camaratenerife.com
Cámara de Comercio de Santiago de Compostela: http://www.camaracompostela.com
Cámara de Comercio de Segovia: http://www.camarasegovia.org
Cámara de Comercio de Sevilla: http://www.camaradesevilla.com
Cámara de Comercio de Soria: http://www.camarasoria.com
Cámara de Comercio de Tarragona: http://www.cambratgn.com
Cámara de Comercio de Tárrega: http://www.cambratarrega.com
Cámara de Comercio de Terrassa: http://www.cambraterrassa.es
Cámara de Comercio de Teruel: http://www.camarateruel.com
Cámara de Comercio de Toledo: http://www.camaratoledo.com
Cámara de Comercio de Torrelavega: http://www.camaratorrelavega.com
Cámara de Comercio de Tortosa: http://www.cambratortosa.com
Cámara de Comercio de Tui: http://www.camaratui.com
Cámara de Comercio de Valencia: http://www.camaravalencia.com
Cámara de Comercio de Valladolid: http://www.cociva.es
Cámara de Comercio de Valls: http://www.cambrescat.es/valls/p-01.htm
Cámara de Comercio de Vigo: http://www.camaravigo.com
Cámara de Comercio de Vilagarcia: http://www.camaravilagarcia.com
Cámara de Comercio de Zamora: http://www.cocicyl.es/Camaras/Zamora/e-informacion.html
Cámara de Comercio de Zaragoza: http://www.camarazaragoza.com

Unión Europea: http://europa.eu.int

anexo II

GLOSARIO DE TÉRMINOS

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos (art. 2.4 R.D. 994/1999).

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (art. 3.e LOPD).

Ámbito normativo coordinado: todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2.º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidos en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos (aptdo. i) Anexo LCE).

Autenticación: procedimiento de comprobación de la identidad de un usuario (art. 2.6 R.D. 994/1999).

Bloqueo de datos: consiste en la identificación y reserva de los datos con el fin de impedir su tratamiento (art. 1.1 R.D. 1332/1994).

Certificación de un prestador de servicios de certificación: es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público (art. 26.1 LFE).

Certificación de dispositivos seguros de creación de firma electrónica: es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma (art. 27.1 LFE).

Certificado electrónico: 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 (art. 6.1 LFE).

Certificados reconocidos: los certificados electrónicos 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 (art. 11.1 LFE).

Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado (art. 3.i LOPD).

Comunicación comercial: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica (aptdo. f) Anexo LCE).

Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen (art. 3.h LOPD).

Consumidor: persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios (aptdo. e) Anexo LCE).

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario (art. 2.8 R.D. 994/1999).

Contrato celebrado por vía electrónica o contrato electrónico: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones (aptdo. h) Anexo LCE).

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos (art. 2.7 R.D. 994/1999).

Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación (art. 2.12 R.D. 994/1999).

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables (art. 3.a LOPD)

Datos de creación de firma: son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica (art. 24.1 LFE).

Datos de verificación de firma: son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica (art. 25.1 LFE).

Destinatario del servicio o destinatario: persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información (aptdo. d) Anexo LCE).

Dispositivo de creación de firma: es un programa o sistema informático que sirve para aplicar los datos de creación de firma (art. 24.2 LFE).

Dispositivo seguro de creación de firma: es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma (art. 24.3 LFE).

Dispositivo de verificación de firma: es un programa o sistema informático que sirve para aplicar los datos de verificación de firma (art. 25.2 LFE).

Documento electrónico: el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente (art. 3.5 LFE).

Documento nacional de identidad electrónico: es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos (art. 15.1 LFE).

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento (art. 3.g LOPD).

Fecha electrónica: el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados (art. 4.1 LFE).

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3.b LOPD).

Firma electrónica: es 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 (art. 3.1 LFE).

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 (art. 3.2 LFE).

Firma electrónica reconocida: la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (art. 3.3 LFE).

Firmante: 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 (art. 6.2 LFE).

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

Identificación: procedimiento de reconocimiento de la identidad de un usuario (art. 2.5 R.D. 994/1999).

Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada (art. 1.5 R.D. 1332/1994).

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos (art. 2.9 R.D. 994/1999).

Órgano competente: todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas (aptdo. j) Anexo LCE).

Prestador de servicios o prestador: persona física o jurídica que proporciona un servicio de la sociedad de la información (aptdo. c) Anexo LCE).

Prestador de servicios de certificación: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica (art. 2.2 LFE).

Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (art. 3.f LOPD).

Profesión regulada: toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias (aptdo. g) Anexo LCE).

Recurso: cualquier parte componente de un sistema de información (art. 2.3 R.D. 994/1999).

Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento (art. 3.d LOPD).

Servicios de la sociedad de la información o servicios: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.

2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.º La gestión de compras en la red por grupos de personas.

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática.

6.º El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994,de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas (aptdo. a) Anexo LCE).

Servicio de intermediación: servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet (aptdo. b) Anexo LCE).

Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (art. 3.c LOPD).

Usuario: sujeto o proceso autorizado para acceder a datos o recursos (art. 2.2 R.D. 994/1999).

anexo III

CLASIFICACIÓN NORMATIVA

NECESARIA	
Nacional	Ley 59/2003, de 19 de diciembre, de firma electrónica (B.O.E. núm. 304, de 20 de diciembre).
	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, (B.O.E. núm. 166, de 12 de julio).
	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. núm. 298, de 14 de diciembre).
	Ley 47/2002, de 19 de diciembre, de reforma de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE, en materia de contratos a distancia, y para la adaptación de la Ley diversas Directivas comunitarias (B.O.E. núm. 304, de 20 de diciembre).
	Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales, en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación (B.O.E. núm. 313, de 31 de diciembre).
	Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información (B.O.E. núm. 185, de 4 de agosto).
Comunitaria	Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (D.O.L. 178, de 17 de julio).
	Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica, (D.O.L. 13, de 19 de enero).
	Directiva 98/27/CE del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores (D.O. L 166, de 11 de junio).
	Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo, relativa a la protección de los consumidores en materia de contratos a distancia (D.O. L 144, de 4 de junio).

CLASIFICACIÓN NORMATIVA

NECESARIA (Continuación)	
Comunitaria	Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23 de noviembre).
	Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201, de 31 dejulio).
Internacional	Ley Modelo de la CNUDMI sobre Comercio Electrónico, 1996.
CONVENIENTE	
Nacional	Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación (B.O.E. núm. 89, de 14 de abril).
	Real Decreto 1828/1999, de 3 de diciembre, por el que se aprueba el Reglamento del Registro de Condiciones Generales de la Contratación (B.O.E. núm. 306, de 23 de diciembre).
	Real Decreto 1133/1997, de 11 de julio, por el que se regula la autorización de las ventas a distancia e inscripción en el Registro de empresas de ventas a distancia (B.O.E. núm. 177, de 25 de julio).
	Real Decreto 1976/1998, de 18 de septiembre, por el que se modifica el Real Decreto 1133/1997, de 11 de julio, por el que se regula la autorización de las ventas a distancia e inscripción en el Registro de empresas de ventas a distancia (B.O.E. núm. 239, de 6 de octubre).
	Orden CTE/662/2003, de 18 de marzo, por la que se aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España (“es” (B.O.E. núm. 73, de 26 de marzo).
Comunitaria	Directiva 93/13/CEE del Consejo, de 5 de abril, sobre las cláusulas abusivas en los contratos celebrados con consumidores (D.O. L 95, de 21 de abril).
	Directiva 2002/65/CE del Parlamento Europeo y del Consejo, de 23 de septiembre, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, y por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE (D.O. L 271, de 9 de octubre).
Internacional	Ley Modelo de la CNUDMI sobre las firmas electrónicas (2001).
OTRA	
Nacional	Ley 60/2003, de 23 de diciembre, de Arbitraje (B.O.E. núm. 309, de 26 de diciembre).
	Real Decreto 636/1993, de 3 de mayo, por el que se regula el sistema arbitral de consumo (B.O.E. núm. 121, de 21 de mayo).
	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (B.O.E. núm. 7, de 8 de enero).
	Ley 34/1988, de 11 de noviembre, General de Publicidad.

CLASIFICACIÓN NORMATIVA

OTRA (Continuación)

Comunitaria	Directiva 2000/46/CE del Parlamento Europeo y del Consejo, de 18 de septiembre, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades (D.O. L 275, de 27 de octubre).
	Recomendación 98/257/CE de la Comisión, de 30 de marzo relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de los litigios en materia de consumo (D.O. L 115, de 17 de abril).
	Recomendación de la Comisión, de 4 de abril de 2001, relativa a los principos aplicables a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo (D.O. L 109, de 19 de abril).
	Directiva 84/450/CEE del Consejo, de 10 de septiembre, sobre publicidad engañosa y publicidad comparativa (DO L 250, de 19 de septiembre).
	Directiva 97/55/CE del Parlamento Europeo y del Consejo, de 6 de octubre, por la que se modifica la Directiva 84/450/CEE sobre publicidad engañosa, a fin de incluir en la misma la publicidad comparativa, (D.O. L 290, de 23 de octubre).
Internacional	Ley Modelo de la CNUDMI sobre arbitraje comercial internacional (1985).

Cámaras

Cámaras de Comercio
www.camaras.org
902 10 00 96

P.V.P.: 15 €