DERECHO E INTERNET

Lorenzo Cotino Hueso
www.cotino.es
www.derechotics.com
Profesor titular de Derecho constitucional
Coordinador especialidad jurídica del
Master Oficial Sistemas y Servicios de la
Sociedad de la Información
(www.uv.es/mastic)
Universidad de Valencia
2010

"Derecho e internet" subprograma OCW, financiación para la elaboración de materiales docentes en formato OCW. , reconocido en Anexo II de la Resolución de 9 de junio de 2010 del Vicerrector de Planificación e Igualdad de la Universidad de Valencia, por la que se resuelve la convocatoria de ayudas a proyectos de innovación educativa para el curso 2010/2011. **www.uv.es/ocw**

CONTENIDO GENERAL

CONTENIDO DETALLADO

I. HISTORIA Y ORGANIZACIÓN DE INTERNET

1. "Los pioneros de Internet" (Scott Griffin)

Este escrito no es más que una traducción libre de la descripción realizada en

http://www.ibiblio.org/pioneers/

, a cargo de Scott Griffin, un estudiante de la licenciatura en periodismo de la Universidad de Carolina del norte. En dicha página puede seguirse un currículum de cada uno de los diez pioneros de la red.

"Puede centrarse en el número de diez las personas cuyo trabajo ha contribuido de forma notable al desarrollo de Internet, aunque éstos no fueron los únicos "pioneros" de la red, sí es cierto que son los únicos individuos cuya contribución ha sido esencialmente significativa: Vannevar Bush, Licklid, Larry Roberts, Paul Baran, Donald Davies, Bob Metcalfe, Douglas Englebart, Vint Cerf, Bob Kahn, Ted Nelson, Tim Berners-Lee.

Durante la Segunda Guerra Mundial, un VANNEVAR BUSH creó un lazo entre el gobierno federal, la comunidad científica americana, y la empresa. Después de la guerra, Vannevar ayudó a institucionalizar este vínculo. Como consecuencia, se crearon organizaciones como la National Science Foundation y la Advanced Research Projects Agency (ARPA). Con ARPA Internet dio sus primeros pasos. Vannevar también escribió "Como podemos pensar" ("As We May Think) en 1945. En este escrito describió todo un bagaje teórico y de disposición orgánica llamado un " memex", el mismo utilizaría un sistema notablemente similar a lo que ahora llamamos el hypertext.

ARPANET

El Advanced Research Projects Agency fue creada por presidente Dwight Eisenhower después de que los soviéticos lazasen el satélite de Sputnik en octubre de 1957. El lanzamiento soviético causó una crisis en confianza americana. ARPA fue formado para asegurarse de que América no sería cogida otra vez de improvisto en la carrera tecnológica. En 1962, J.c.r. LICKLID fue a trabajar para ARPA. Licklider, psicólogo e informático, creía que los ordenadores se podrían utilizar para mejorar al

pensamiento humano y sugirió que una red de ordenadores permitiría que los investigadores de ARPA pudiesen comunicar eficientemente la información entre sí. Licklider no construyó realmente su red propuesta, pero su idea permaneció viva cuando dejó ARPA en 1964,

BOB TAYLOR era el director de la oficina de las técnicas de la tratamiento de la información de ARPA (IPTO) entre 1966 y 1969. Bob, deseó encontrar una manera eficiente de permitir que los varios contratistas de IPTO compartiesen recursos que computaban. Él recogió la vieja idea de Licklider de una red y empleó a LARRY ROBERTS para dirigir el proyecto. Roberts sería el arquitecto principal de una nueva red de ordenadores que sería conocida como el ARPANET. Así los principios del Internet siguieron en curso.

La configuración de ARPANET se fundamentó básicamente en las ideas de PAUL BARAN, co-inventor de un nuevo sistema conocido como "packet-switching" (la conmutación de conjuntos de bits). (Un informático británico, DONALD DAVIES, independientemente mejoró con sus propias teorías la conmutación de conjunto de bits). Paul Baran también sugirió que la red estuviese diseñada como red distribuida. Este diseño, que incluyó un alto nivel de redundancia, haría la red más robusta en el caso de un ataque nuclear. Aquí fue probablemente de donde procede el mito que Internet fue creado como red de comunicaciones para el acontecimiento de una guerra nuclear. Como una red distribuida, ARPANET era definitivamente robusta, y habría podido soportar posiblemente un ataque nuclear, pero la principal meta de sus creador era facilitar comunicaciones normales entre los investigadores

ARPANET conectó grandes ordenadores centrales, por medio de routers, conocidos como "Interface Message Processors " procesadores del mensaje del interfaz (IMPs). El 1 de septiembre de 1969, el primer IMP llegó UCLA (la prestigiosa universidad de California). Un mes más tarde el segundo fue instalado en Stanford, luego la Universidad de Santa Barbara y luego la universidad de Utah.

El verdadero Internet

El ARPANET continuó creciendo. La tecnología del trabajo en red continuó convirtiéndose con personas como BOB METCALFE, que inventó Ethernet, y DOUGLAS ENGLEBART, inventor del ratón entre otras cosas, dio cobertura a la tecnología necesaria. Otras redes de ordenadores, como ALOHANET y la red conectada basada en los satélites SATNET de Hawaii, comenzaron a originarse. Pronto fueron muchas las redes diversas de ordenadores en todo el mundo, pero no podrían comunicarse una con otras porque utilizaban diversos protocolos o estándares para los datos que transmitían. Entonces en 1974, VINT CERF (conocido usualmente como el " padre del Internet "), junto con BOB KAHN, generaron un nuevo protocolo, TCP ("Transmission Control Protocol"), protocolo de control de transmisión), que se convirtió en el estándar valido. La puesta en práctica del TCP permitió que las varias redes conectaran en un " Internet verdadero. "

Internet llegó a ser extensamente popular en el ordenador y las comunidades de investigación científicas. En los años 80 la mayoría de las universidades y de las instituciones investigación-research-oriented tenían ordenadores que fueron conectados con Internet.

El World Wide Web (WWW)

En los años 70, TED NELSON acuñó el término "hypertexto" para describir un sistema para la conexión no lineal de los documentos, sistema inspirado directamente en trabajos de Vannevar Bush. Usando hypertext, en 1990 TIM BERNERS-LEE creó una nueva manera de obrar recíprocamente con Internet en ya mundialmente conocido WWW. Su sistema hacía mucho más fácil compartir y encontrar datos en la red. Así, el World Wide Web fue aumentado más a fondo por otros que crearon nuevos software y tecnologías para hacerlo más funcional. Por ejemplo, el Marc Andreesen creó un nuevo browser llamado Mosaic y después lideró al equipo que creó el Netscape Navigator. El World Wide Web permitió la extensión de la red y continúa hoy creciendo y cambiando de maneras a veces imprevisibles."

2. Una aproximación al inventor de la worl wild web: Tim Berners-Lee

Se recomienda su obra, recientemente editada en España BERNERS-LEE, Tom, *Tejiendo la Red*, Siglo XXI, Madrid, 2000.

Noticia de *El Mundo, a cargo de José Luis de Vicente, que me permito reproducir este trabajo de*

http://www.elmundo.es/navegante/personajes/bernerslee.html

Para profundizar sobre Tim Berners-Lee, ver su página

http://www.w3.org/People/Berners-Lee/Overview.html

Sin ninguna duda, Berners-Lee es el responsable más directo e inmediato de que usted pueda estar leyendo este artículo ahora mismo. Antes de 1990, Internet no era este inmenso espacio que podemos cruzar en una dirección y otra en cuestión de segundos con sólo pulsar un enlace; más bien se parecía a un archipiélago de miles de islas inconexas. No existían los buscadores, no se podía integrar imágenes y textos con facilidad en la pantalla, y pretender obtener la información que nos interesaba no era muy distinto de encontrar la proverbial aguja en el pajar.

Entra Tim Berners-Lee, un científico británico del Laboratorio Europeo de Física de Partículas (CERN) decidido a desarrollar un método eficiente y rápido para intercambiar datos entre la comunidad científica. Para ello, combinó dos tecnologías ya existentes (el hipertexto y el protocolo de comunicaciones de Internet), creando un nuevo modelo de acceso a la información intuitivo e igualitario. Las famosas tres W han hecho posible que aprender a utilizar la Red sea algo al alcance de cualquiera.

Actualmente, Tim Berners-Lee está al frente del World Wide Web Consortium, la organización que coordina estándares y añade nuevas funcionalidades a la Web. Por encima de todo, sigue promoviendo su visión de la www como una fuerza que incentive el cambio social y la creatividad del individuo. La revista Time lo escogió como una de las 100 personalidades más importantes del siglo XX.

3. Una breve cronología de la red

Este material está disponible en

http://www.alfinal.com/Temas/internet.htm

1. Breve historia de Internet

Cuando las computadoras comenzaron a conectarse unas con otras a traves de W.A.N. (Wide Area Networks) tales como ARPANET hacia 1960, fue necesariauna forma de identificación para acceder a los sistemas.

Al principio las redes estaban compuestas de solo unas pocas computadoras aosciadas con el Departamento de Defensa y otras instituciones. Cuando el número de computadores creció, se hizo necesario un sistema más eficiente para regular y mantener los caminos de los dominios a traves de la red.

En 1972, el Sistema de Agencias de Información de Defensa creo el IANA o Autoridad de asignación de números de Internet, responsable para asignar una dirección única a cada computador conectado a Internet.

En 1973, el IP o protocolo de Internet se volvió un standard por el cual todas las computadoras de la red podían ser ubicadas. Luego con la creación de los correos electrónicos el crecimiento se hizo geométrico.

En 1984 se creó en Winsconsin el primer 'name server' con el cual no se necesitó más conocer el path de localización de un computador, el cual es usado hasta nuestros días. Un año después el DNS Domain Name Server fue implementado y los sufijos .com, .net y .org añadidos.

En 1990, internet devino comercial y fue seguida por la aparición en escena de la WWW (world wide web) por obra de Tim Berners-Lee y CERN. Inicialmente el registro fue gratis, subsidiada por la Fundación Nacional de la Ciencia a traves del IANA, pero en 1992 IANA y NSF se unieron creando InterNic (a la que está vinculada, por su parte, la NCS –concesionaria de los EEUU), .

En 1995 se acabó el subsidio e Internic comienza a cobrar $100 por cada registro por dos años. En 1998 se permite a los privados la oferta de inscripciones de dominios. ICANN se formalizó como compañía en 1998.

Esta corporación privada sin fines de lucro formada por una coalición de empresas con intereses de negocios en internet a lo largo de lmundo es reconocida como la entidad de consenso global para coordinar la administración tecnica de los DNS, su ubicación IP, la asignación de protocolos y la administración del sistema raíz del server.Uno de sus principales objetivos es el espiritu de libre competenciaen la industria de los dominios, ya que ha acreditado a varias compañias para agregar dominios globales en su base de datos.

Este es un sistema de registración compartida. Actualmente se estima en 19 millones de nombres de dominio registrados y un promedio de 40.000 registros diarios. La accesibilidad, libertad y competencia son sus únicas reglas.

2. Pequeña historia de Internet, por Bruce Sterling

(bruces@well.sf.ca.us)
Traducción de Antonio Montesinos
(a.monte@jet.es)
Publicado originalmente en español en Alejandría:
http://www.web.sitio.net/faq
Nota del traductor:

Este texto refleja brevemente y de manera muy clara la historia de Internet y las herramientas más usadas en el momento en que se escribió el artículo (1992). Es un texto muy clarificador, sobre todo para aquellos que desconocen los orígenes de la red. La única aclaración que hay que hacer sobre él es que las cifras que aparecen hay que aplicarlas al año 1992. Cuando se mencionan el número de ordenadores conectados, usuarios que utilizan la red, los distintos grupos de noticias, precios, etc. hay que hacer constar que esas cifras corresponden a ese año y que actualmente esas cantidades han variado mucho. Por lo demás la calidad del texto es excelente.

Freeware literario -- Prohibido su uso comercial

Extraído de LA REVISTA DE FANTASÍA Y CIENCIA FICCIÓN, Febrero de 1993.

F&SF, Box 56, Cornwall CT 06753 $26/yr USA $31/yr other

F&SF Columna sobre ciencia 5

"Internet"

Hace unos treinta años, la RAND Corporation, la primera fábrica de ideas de la América de la guerra fría, se enfrentó a un extraño problema estratégico. ¿Cómo se podrían comunicar con éxito las autoridades norteamericanas tras una guerra nuclear?

La América postnuclear necesitaría una red de comando y control enlazada de ciudad a ciudad, estado a estado, base a base. Pero sin importar cómo esa red estuviera de protegida, sus líneas y equipos siempre serían vulnerables al impacto de bombas atómicas. Un ataque nuclear reduciría cualquier red imaginable a pedazos.

¿Cómo sería controlada esa red? Cualquier autoridad central, cualquier núcleo de red centralizado sería un objetivo obvio e inmediato para un misil enemigo. El centro de la red sería el primer lugar a derribar.

La RAND le dio muchas vueltas a este difícil asunto en secreto militar y llegó a una solución atrevida. La propuesta de la RAND se hizo pública en 1964. En primer lugar, la red *no tendría autoridad central*. Además, sería *diseñada desde el principio para operar incluso hecha pedazos.*

Los principios eran simples. Se asumiría que una red era poco fiable en cualquier momento. Se diseñaría para trascender su propia falta de eficacia. Todos los nodos en la red serían iguales entre sí, cada nodo con autoridad para crear, pasar y recibir mensajes. Los mensajes se dividirían en paquetes, cada paquete dirigido por separado. Cada paquete saldría de un nodo fuente específico y terminaría en un nodo destino. Cada paquete recorrería la red según unos principios particulares.

La ruta que tome cada paquete no tendría importancia. Solo contarían los resultados finales. Básicamente, el paquete sería lanzado como una patata de un nodo a otro, más

o menos en dirección a su destino, hasta acabar en el lugar adecuado. Si grandes porciones de la red fueran destruidas eso simplemente no importaría; los paquetes permanecerían en la red en los nodos que hubieran sobrevivido. Este sistema de envío tan arbitrario podría parecer "ineficiente" en el sentido usual del término (especialmente comparado con, por ejemplo, el sistema telefónico).

Durante los 60, este intrigante concepto de red de conmutación de paquetes descentralizada y a prueba de bombas caminó sin rumbo entre el RAND, el MIT (Masachussets Institute of Technology) y UCLA (University of California in Los Angeles). El Laboratorio Nacional de Física (National Physical Laboratory) de Gran Bretaña preparó la primera red de prueba basada en estos principios en 1968. Poco después, la Agencia de Proyectos de Investigación Avanzada del Pentágono (ARPA) decidió financiar un proyecto más ambicioso y de mayor embergadura en los Estados Unidos. Los nodos de la red iban a ser superordenadores de alta velocidad (o lo que se llamara así en aquel momento). Eran máquinas poco usuales y de mucho valor y que estaban necesitadas de un buen entramado de red para proyectos nacionales de investigación y desarrollo.

En el otoño de 1969 el primero de esos nodos fue instalado en UCLA. En diciembre de ese año había cuatro nodos en la pequeña red, que se llamó ARPANET después de que fuera promocionada por el Pentágono. Los cuatro ordenadores podían transferir información sobre líneas dedicadas de alta velocidad. Incluso podían ser programados remotamente desde otros nodos. Gracias a ARPANET, científicos e investigadores podían compartir las facilidades de otros ordenadores en la distancia. Era un servicio muy útil ya que el tiempo de proceso de los ordenadores en los 70 era algo muy codiciado. En 1971 había quince nodos en ARPANET; en 1972, treinta y siete. Todo iba perfecto.

En su segundo año de operatividad, sin embargo, algo extraño se hizo patente. Los usuarios de ARPANET habían convertido la red en una oficina de correos electrónica de alta velocidad subvencionada federalmente. La mayor parte del tráfico de ARPANET no era el proceso de datos a largas distancias. En vez de eso, lo que se movía por allí eran noticias y mensajes personales. Los investigadores estaban usando ARPANET para colaborar en proyectos, intercambiar notas sobre sus trabajos y, eventualmente, chismorrear. La gente tenía sus propias cuentas personales en los ordenadores de ARPANET y sus direcciones personales de correo electrónico. No es que sólo utilizaran ARPANET para la comunicación de persona a persona, pero había mucho entusiasmo por esta posibilidad -- mucho más que por la computación a larga distancia.

Eso no pasó mucho antes del invento de las listas de distribución, una técnica de emisión de información por ARPANET mediante la cual un mismo mensaje se podía enviar automáticamente a una gran cantidad de subscriptores. Es interesante que una de las primeras listas de distribución masivas se llamara "Amantes de la Ciencia Ficción" (SF- LOVERS). Discutir sobre ciencia ficción en la red no tenía nada que ver con el trabajo y eso enfadaba a muchos administradores de sistema de ARPANET, pero eso no impediría que la cosa siguiera.

Durante los 70, ARPANET creció. Su estructura descentralizada facilitó la expansión. Contrariamente a las redes standard de las empresas, la red de ARPA se podía acomodar a diferentes tipos de ordenador. En tanto en cuanto una máquina

individual pudiese hablar el lenguaje de conmutación de paquetes de la nueva y anárquica red, su marca, contenidos e incluso su propietario eran irrelevantes.

El estándar de comunicaciones de ARPA era conocido como NCP, "Network Contro Protocol", pero según pasaba el tiempo y la técnica avanzaba, el NCP fue superado por un estándar de más alto nivel y más sofisticado conocido como TCP/IP. El TCP o "Trasmision Control Protocol," convierte los mensajes en un caudal de paquetes en el ordenador fuente y los reordena en el ordenador destino. El IP, o "Internet Protocol", maneja las direcciones comprobando que los paquetes caminan por múltiples nodos e incluso por múltiples redes con múltiples estándards -- no sólo ARPA fue pionera en el stándar NCP, sino también Ethernet, FDDI y X.25.

En 1977, TCP/IP se usaba en otras redes para conectarse a ARPANET. ARPANET estuvo controlada muy estrictamente hasta al menos 1983, cuando su parte militar se desmembró de ella formando la red MILNET. Pero el TCP/IP las unía a todas. Y ARPANET, aunque iba creciendo, se convirtió en un cada vez más pequeño barrio en medio de la vasta galaxia de otras máquinas conectadas.

Según avanzaban los 70 y 80, distintos grupos sociales se encontraban en posesión de potentes ordenadores. Era muy fácil conectar esas máquinas a la creciente red de redes. Conforme el uso del TCP/IP se hacía más común, redes enteras caían abrazadas y adheridas a Internet. Siendo el software llamado TCP/IP de dominio público y la tecnología básica descentralizada y anárquica por propia naturaleza, era muy difícil parar a la gente e impedir que se conectara. De hecho, nadie quería impedir a nadie la conexión a esta compleja ramificación de redes que llegó a conocerse como "Internet".

Conectarse a Internet costaba al contribuyente muy poco o nada desde que cada nodo era independiente y tenía que arreglárselas con la financiación y los requerimientos técnicos. Cuantos más, mejor. Como la red telefónica, la red de ordenadores era cada vez más valiosa según abarcaba grandes extensiones de terreno, gente y recursos.

Un fax solo es útil si "alguien más" tiene un fax. Mientras tanto no es más que una curiosidad. ARPANET, también, fue una curiosidad durante un tiempo. Después la red de ordenadores se convirtió en una necesidad importante.

En 1984 la Fundación Nacional para la Ciencia (National Science Foundation - NSF) entró en escena a través de su Oficina de Computación Científica Avanzada (Office of Advanced Scientific Computing). La nueva NSFNET supuso un paso muy importante en los avances técnicos conectando nuevas, más rápidas y potentes supercomputadoras a través de enlaces más amplios, rápidos, actualizados y expandidos según pasaban los años, 1986, 1988 y 1990. Otras agencias gubernamentales también se unieron: NASA, los Institutos Nacionales de la Salud (National Institutes of Health), El Departamento de Energía (Departament of Energy), cada uno manteniendo cierto poderío digital en la confederación Internet.

Los nodos de esta creciente red de redes se dividían en subdivisiones básicas. Los ordenadores extranjeros y unos pocos americanos eligieron ser denominados según su localización geográfica. Los otros fueron agrupados en los seis "dominios" básicos de Internet: gov, mil, edu, com, org y net. (Estas abreviaturas tan sosas pertenecen al estándar de los protocolos TCP/IP). Gov, Mil y Edu definen al gobierno, militares e instituciones educativas, las cuales fueron, por supuesto, las pioneras de la ARPANET que comenzó como un experimento de alta tecnología en seguridad nacional. Com, sin embargo, definía a instituciones "comerciales", que enseguida entraron a la red como

toros de rodeo rodeadas por una nube de entusiastas "orgs" sin ánimo de lucro. (Los ordenadores tipo "net" servían como pasarelas entre redes).

La red ARPANET propiamente dicha expiró en 1989 como víctima feliz de su éxito abrumador. Sus usuarios apenas se dieron cuenta, pero las funciones de ARPANET no solo continuaron sino que mejoraron firmemente. El uso del estándar TCP/IP para redes es ahora algo global. En 1971, hace 21 años, sólo había cuatro nodos en la red ARPANET. Hoy existen decenas de miles en Internet esparcidos por cuarenta y dos países y muchos más que se conectan cada día. Tres millones de personas, posiblemente cuatro, usan esta gigantesca madre- de-todas-las-redes.

Internet es especialmente popular entre los científicos y es probablemente su instrumento más importante de finales del siglo XX. Las posibilidades de acceso tan potentes y sofisticadas que ofrece a datos específicos y a la comunicación personal ha elevado la marcha de la investigación científica enormemente.

El índice de crecimiento de Internet a comienzo de los 90 es espectacular, casi feroz. Se extiende más rápidamente que los teléfonos móviles y que el fax. El año pasado Internet crecía a un ritmo del 20% mensual. El número de ordenadores con conexión directa al TCP/IP se ha estado doblando anualmente desde 1988. Internet se está desplazando de su origen militar y científico a las escuelas de enseñanza básica e institutos, al mismo tiempo que a bibliotecas públicas y el sector comercial.

¿Por qué la gente quiere estar "en Internet"? Una de las principales razones es simplemente la libertad. Internet es un raro ejemplo de anarquía verdadera, moderna y funcional. No existe "Internet, S.A." No hay censores oficiales, ni jefes, ni junta directiva, ni accionistas. En principio, cualquier nodo puede hablar de igual a igual a otros nodos siempre que obedezcan las leyes del protocolo TCP/IP, leyes que no son políticas sino estrictamente técnicas. (Ha existido controversia sobre el uso comercial de Internet, pero esta situación está cambiando según los negocios proporcionan sus propios enlaces y conexiones).

Internet también es una ganga. Internet en conjunto, a diferencia del sistema telefónico, no cuesta dinero según las distancias. Y a diferencia también de la mayoría de las redes comerciales, no se cobra por tiempo de conexión. De hecho, "Internet" de por sí, que ni siquiera existe como una entidad, no cobra "nada" por nada. Cada grupo de gente que accede a Internet es responsable de su propia máquina y de su propio trozo de línea.

La "anarquía" de Internet puede parecer extraña o incluso poco natural, pero tiene cierta profundidad y sentido. Es como la "anarquía" del idioma inglés. Nadie alquila el inglés y nadie lo posee. Como anglo-parlante, depende de ti aprender hablar inglés correctamente y usarlo para lo que quieras (aunque el gobierno proporciona fondos para ayudarte a que aprendas a leer y escribir algo). Aunque mucha gente se gana la vida usando, explotando y enseñando inglés, el "inglés" como institución es una propiedad pública, un bien común. Mucho de eso ocurre con Internet. ¿Mejoraría el inglés si "Idioma Inglés, S.A." tuviera un consejo de administración con su director o ejecutivo al frente, un presidente y una asamblea? Probablemente exsitirían muchas menos palabras en el idioma inglés, y muchas menos nuevas ideas.

La gente en Internet siente que se trata de una institución que se resiste a la institucionalización. El interés pertenece a todos y a nadie.

A pesar de esto, hay quién tiene intereses en Internet. Los negociantes quieren que Internet tenga una base financiera. Los gobernantes la quieren más regulada. Los

académicos la quieren para fines de investigación. Los militares para la seguridad. Y así muchos más.

Todas estas fuentes de conflicto permanenen en torpe equilibrio, e Internet, hasta ahora, se mantiene en próspera anarquía. Antes, las líneas de alta velocidad de la NSFnet eran conocidas como la "espina dorsal de Internet" (Internet Backbone), y sus propietarios podían señorearse con el resto de Internet; pero hoy existen "espinas dorsales" en Canadá, Japón y Europa, e incluso algunas privadas para el tráfico comercial. Hoy, incluso ordenadores domésticos privados pueden convertirse en nodos de Internet. Se pueden llevar bajo el brazo. Pronto, quizás, en la muñeca.

Pero, ¿Qué se *hace* en Internet? Básicamente, cuatro cosas: correspondencia, grupos de discusión, computación a larga distancia y transferencia de archivos. El correo de Internet es el correo electrónico (e-mail), mucho más rápido que el correo postal americano, que es llamado despectivamente por los usuarios de Internet como "correo caracol" (snail mail). El correo en Internet es algo como el fax. Es texto electrónico, y no tienes que pagar por él (al menos directamente) y es a escala global. Por correo electrónico se puede mandar software y algunos tipos de imágenes comprimidas. Se está trabajando en nuevas formas de correo electrónico.

Los grupos de discusión, o "newsgroups", son un mundo aparte. Este mundo de debate y argumentaciones se conoce como "USENET". USENET es de hecho diferente a Internet. USENET es como una multitud ondulante de gente chismosa y con ganas de información que se mueve por Internet en busca de barbacoas de patio trasero. USENET no es tanto una red física como un conjunto de convenciones. En cualquier caso, ahora existen 2.500 grupos de discusión separados en USENET y sus mensajes generan unos 7 millones de palabras al día. Naturalmente se habla mucho sobre ordenadores en USENET, pero la variadad de temas sobre los que se habla es enorme, creciendo estos continuamente. En USENET se distribuyen varias publicaciones electrónicas gratuitas de manera periódica.

Estos grupos y el correo electrónico están disponibles fácilmente, incluso fuera del corazón de Internet. Se puede acceder a ellos a través de las líneas de teléfono normales, desde otras redes como BITnet, UUCP y Fidonet. Los últimos servicios de Internet, computación a larga distancia y tranferencia de archivos, requieren de conexión directa usando TCP/IP.

La computación a larga distancia fue algo pensado para ARPANET y aún se usa mucho, al menos por algunos. Los programadores puenden mantener sus cuentas abiertas en poderosos super-ordenadores y ejecutar allí sus programas o crear otros nuevos. Los científicos pueden usar potentes ordenadores desde otros continentes. Las bibliotecas ofrecen sus catálogos electrónicos para que se busque en ellos gratuitamente. Enormes catálogos en CD-ROM están disponibles a través de este servicio. Y existe mucho software gratuito al mismo tiempo.

La tranferencia de ficheros permite a los usuarios acceder a máquinas remotas y tomar de ellas programas o textos. Muchos ordenadores de Internet - unos dos mil o más - permiten que se acceda a ellos de manera anónima y que la gente use sus archivos de manera gratuita. Esto no es algo trivial, ya que libros enteros se pueden transferir en cuestión de minutos. Hoy, en 1992, existen más de un millón de ficheros públicos disponibles a quién los quiera utilizar (y otros millones disponibles a gente con autorización). La transferencia de ficheros por Internet se está convirtiendo en una nueva forma de publicación, en la que el lector copia electrónicamente el texto que

desee en la cantidad que quiera y de forma gratuita. Nuevos programas de Internet, como "archie", "gopher" y "WAIS" se han desarrollado para catalogar y explorar esa cantidad de material.

Esta Internet sin cabeza, anárquica y con millones de tentáculos se está extendiendo como el pan de molde. Cada ordenador con la potencia suficiente es una espora potencial de Internet y hoy los ordenadores se venden a menos de 2.000 dólares y están disponibles en todo el mundo. La red ARPA, diseñada para asegurar el control de una sociedad desolada después de un holocausto nuclear, ha sido sobrepasada por su hija mutante, Internet, que está a fuera de control a conciencia y se expande exponencialemente por la aldea global de la post guerra fría. La expansión de Internet en los 90 se parece a la que sufrió la informática personal en los 70, aunque esta es más rápida y más importante. Más importante, quizás, porque da a los ordenadores personales una imagen de algo barato, de fácil acceso y con posibilidades de almacenaje a una escala realmente planetaria.

El futuro de Internet pasa por ser más grande y con velocidades exponencialmente mayores. La comercialización de Internet es un tema candente hoy día, donde se promete cualquier tipo de comercialización salvaje de la información. El gobierno federal, agradecido por este éxito inesperado, aún tiene mucho que decir en esto. La NREN (National Research and Educational Network - Red Nacional de Educación e Investigación), fue aprobada en el otoño de 1991 como un proyecto a cinco años y con un presupuesto de dos billones de dólares para que la red troncal de Internet fuera actualizada. NREN será unas 50 veces más rápida que la red más rápida de hoy día permitiendo la transferencia de la Enciclopedia Británica en un segundo. Las redes de ordenadores permitirán gráficos animados en 3-D, enlaces de radio y teléfonos móviles a ordenadores portátiles, fax, voz y televisión de alta definición. ¡Un circo global multimedia!

O al menos así se espera - y se planea. La Internet real del futuro debe soportar pocos parecidos con los planes de hoy. Preveer las cosas nunca ha tenido mucho que ver con el rápido desarrollo de Internet. Después de todo, Internet se parece muy poco a aquellos sombríos planes del RAND para el post-holocausto. Esto resulta ser una sutil y feliz ironía.

¿Cómo se accede a Internet? Bien -- si no se tiene un ordenador y un modem, hay que hacerse con uno. El ordenador puede actuar como una terminal y se puede usar una línea de teléfonos ordinaria para conectarse a una máquina enganchada a Internet. Simplemente esto puede hacer que se tenga acceso a los grupos de discusión y a una dirección de correo electrónico propia. Merece la pena tener estos servicios -- aunque sólo con el correo y las noticias no se está del todo "en Internet".

Si está vd. en un campus, la universidad puede que tenga "acceso directo" a líneas TCP/IP de Internet de alta velocidad. Hágase con una cuenta de Internet en un ordenador del campus y será capaz de utilizar los servicios de computación remota y la transferencia de archivos. Algunas ciudades como Cleveland proporcionan acceso gratuito a la red. Las empresas tienen cada vez más posibilidades de acceso y están deseando vender esos accesos a sus clientes. La cuota estándar es de unos 40 dólares al mes -- más o menos como el servicio de TV por cable.

Según avancen los 90, encontrar acceso a Internet será mucho más fácil y barato. Su facilidad de uso también mejorará del salvaje interface UNIX del TCP/IP a otros muchos más intuitivos y cómodos para el usuario, eso es una buena noticia. Aprender

Internet ahora, o al menos aprender sobre Internet, es para entendidos. Cuando cambiemos de siglo la "cultura de redes", tal como la "cultura de los ordenadores" antes de esta se verá forzada a introducirse en el ámbito de su vida.

Más lecturas sobre este tema:

The Whole Internet Catalog & User's Guide by Ed Krol. (1992) O'Reilly and Associates, Inc. Una clara introducción sin tecnicismos al negocio de la cultura de redes. Muchos libros sobre ordenadores intentan ser simpáticos, este libro lo consigue.

The Matrix: Computer Networks and Conferencing Systems Worldwide. by John Quarterman. Digital Press: Bedford, MA. (1990). Un compendio masivo y técnico que detalla el sorprendente alcance y complejidad de nuestro recién interconectado planeta.

The Internet Companion by Tracy LaQuey with Jeanne C. Ryer (1992) Addison Wesley. Exacta guía de educación para Internet con anécdotas de experiencias de la vida real en Internet. Prefacio del senador Al Gore.

Zen and the Art of the Internet: A Beginner's Guide by Brendan P. Kehoe (1992) Prentice Hall. Breve pero útil guía con buenos consejos sobre como utilizar las máquinas para hacerse con información. Esta guía refleja la maravillosa posibilidad de estar en en la red de manera gratuita. Yo hago lo mismo con mis artículos de F&SF, incluyendo por supuesto este.

Mi dirección de correo electrónico en Internet es:

bruces@well.sf.ca.us.

4. Organización de la red, ICANN

1. Qué es ICANN

El ICANN es una entidad sin fines de lucro, internacional y representativa de la Comunidad Internet. Su objetivo es Gobernar las políticas sobre Nombres de Dominios, Direcciones IP y

Protocolos. Esta Corporación fue creada por iniciativa del Gobierno de los Estados Unidos, en un proceso que se inició en 1998 y que tenía por objeto el pasar a manos "no estatales" e internacionales las funciones que hasta ese momento eran llevadas a cabo bajo su responsabilidad.

Se denominan miembros At Large del ICANN a aquellos individuos con interés sobre los temas que hacen a la fijación de políticas

sobre Nombres de Dominios, Direcciones IP y Protocolos.

Tiene como cuerpo de gobierno un Directorio compuesto por 18 personas. Se inicia ahora la suscripción de miembros individuales

(no implica costo alguno asociarse), puesto que en agosto, más tardar setiembre, se procederá a elegir un Director por cada una de las 5 Regiones Geográficas que la Entidad ha establecido.

Durante el mes de Septiembre del corriente, todos los miembros At Large, podrán votar por los candidatos a integrar el Directorio del ICANN, y lo harán utilizando estos tres elementos (número, password y PIN).

En la primera elecciones a llevar a cabo en setiembre, cada región elegirá un Director (cinco en total). En una etapa posterior se elegirán otros cuatro Directores, entre los que no podrá haber más de uno por región.

ICANN: LA NUEVA ENTIDAD GLOBAL QUE COORDINARA INTERNET

http://www.empresas-galicia.com/icann/index.htm

http://www.empresas-galicia.com/icann/iana_icann.htm

ICANN es una entidad de caracter global, que con el beneplácito del gobierno USA, pasará a administrar (gobernar segun muchas opiniones) los aspectos gobernables de Internet. Los mismos aspectos que, en los origines de Internet, gestionaba otra entidad conocida como IANA (Internet Asigned Numbers Authority).

Dichos aspectos, se corresponden con los llamados "parametros coordinables de Internet". Su gestiónn es esencial para el buen funcionamiento de la Red. Normalmente se les clasifica en los cuatro grupos operacionales siguientes:

La distribución de Numeros IP.

El Sistema de Dominios de Nombres (sistema DNS).

La coordinación de parametros asociados con el Protocolo TCP/IP.

La gestion de los llamados "Root Servers·" (Servidores Raiz - donde residen los punteros hacia los servidores DNS de los ".com", ".org", ".es", etc.).

El gobierno de internet: de IANA a ICANN

A. Gonzalez (Miembro del MITF de ICANN)

INTRODUCCION

En 1993, cuando impartí la primera conferencia, en Galicia, acerca de Internet, dije que la palabra Internet se haría tan popular como el fax. Los pocos asistentes en la sala de conferencias de GALITRONICA '93, ni se inmutaron. La idea les resbaló sobre su cerebro como si el conferenciante acabase de decir una tontería.

Hoy día todos reconocemos la popularidad e importancia de Internet en el campo de las telecomunicaciones. Dentro de esta popularidad, se ha extendido la idea de que Internet no tiene gobierno. Pero la realidad es que existe una entidad de gobierno y su evolución actual es de suma importancia para toda la comunidad internética global.

Efectivamente, a escala global y en paises democráticos, nadie controla o puede impedir, la cantidad y tipo de contenidos que se volcan sobre la Red a diario. Tampoco nadie regula quien puede conectarse a la Red y a quien se le deba denegar dicho derecho. En tal sentido la Red no tiene gobierno. Es libre y para todos. Pero hay otros aspectos, que sí necesitan ser controlados. Caso de no ser administrados por una entidad (o gobierno) central, Internet dejaría de funcionar. Por ejemplo, si alguien cambiase el valor (pointer) que, en los llamados "root servers", indica que ".es" se asocia con direcciones Internet españolas, para la mayoría de los internautas del resto del mundo, la Internet en España habria desaparecido del mapa (para alcanzar "hosts" en España se necesitaría saber su IP).

s necesaria y existe una entidad que gobierna Internet. Dicha entidad, está todavía bajo control del gobierno USA. Sus decisiones afectan y seguirán afectando a toda la comunidad internética global. Recientemente, el gobierno USA, ha decidido transferir la gobernabilidad de Internet a una entidad internacional de nueva creación. Un nombre ya existe. Se llamará ICANN (Internet Corporation for Assigned Numbers and Names).

La creación de dicha entidad, es parte de un proceso iniciado en 1998, y que está actualmente en marcha. Curiosamente, a pesar de su enorme importancia para la evoluciónn de Internet y siendo un proceso abierto, está ocurriendo a espaldas de la mayoría de los internautas. La razón: son muy pocos los que le están prestando la atención debida.

Los aspectos gobernables de Internet (aquellos que en su día serán gestionados por ICANN), se corresponden con los llamados "parametros coordinables de Internet". Su gestiónn es esencial para el buen funcionamiento de la Red. Normalmente se les clasifica en los cuatro

grupos operacionales siguientes:

1.La distribución de Numeros IP.

2.El Sistema de Dominios de Nombres (sistema DNS).

3.La coordinación de parametros asociados con el Protocolo TCP/IP.

4.La gestion de los llamados "Root Servers·" (Servidores Raiz - donde residen los punteros

hacia los servidores DNS de los ".com", ".org", ".es", etc.).

Un poco de historia

Cuando Internet era pequeña, un reducido grupo de pioneros internéticos que operaba bajo el nombre de IANA (Internet Asigned Numbers Authorithy), se encargaba de la gestión de los parametros coordinables. Era el único gobierno de Internet. Lo presidía el "dios de los números - IP" (el fallecido Jon Postel).

Conforme la Red creció y empezaron a predominar los intereses comerciales, sobre los cientifico, académico y militar de sus origines, el Congreso USA decidió (en 1992) que era necesario comercializar Internet. A tal fin puso a concurso público la gestión de los Servidores Raiz y la de los nombres a nivel gSLD (genéricos de segundo nivel: bajo ".com", ".net" y

".org"). Dicho concurso lo ganó NSI (Network Solutions Inc.).

Inicialmente NSI era una pyme pero, por detrás, estaba el apoyo/interés de un grupo de gran influencia en el gobierno USA. Ello le permitió no solo crecer sino que ademas le permitió actuar de forma abusiva, mientras se embolsaba millones de dolares en beneficios

(procedentes tanto de los solicitantes de registro como del gobierno USA). Su forma de

actuar, propició en gran parte la conocida "guerra de nombres".

Un gobierno internacional en formación: ICANN

En 1996, un año antes del final del contracto de NSI y el gobierno USA , varios grupos liderados por el ISOC (Internet SOCiety) trataron de evitar que se le renovase el contracto. En preparación para ello, iniciaron el proceso de creación de un consorcio/comité internacional (conocido como CORE). que se encargaría de las funciones de gestión que hasta ese momento habian corrido a cargo de NSI. Sin

embargo, el poder lobista de NSI consiguió impedirlo. En enero de 1998, el gobierno USA publicaba el llamado "Green Paper" donde invitaba a la comunidad internética global a opinar acerca de la creación de una entidad internacional de gobierno de Internet. De esta forma se anulaba el proceso CORE. Desparecía la posibilidad de que los uevos dominios de nivel superior (".firm", ".shop", ".web",

".arts",etc.) entrasen en circulación y al mismo tiempo permitía que NSI siguiese embolsandose sus millones.

Una vez recibidas opiniones pro/contra de todo el mundo (un total de 650, entre ellas 3 desde España (una desde Galicia por el autor del presente artículo), el gobierno USA publicó sus conclusiones en el llamado "White Paper" donde se exponían los principios a los que debian

de conformarse los estatutos de ICANN (la nueva entidad internacional de gobierno de Internet).

Finalmente, en agosto de 1998, se inició el proceso de creación de ICANN. A nivel de junta directiva constará con un presidente y 18 directores. De estos, 9 se eligirán de entre la comunidad internética mundial (los llamados "Directors At Large"), y los 9 restantes serán elegidos por las llamadas SOs (Supporting Organizations) quienes a su vez representan a los grupos de interés asociados con los parametros coordinables. A fin de conseguir la mas amplia diversidad geográfica de participación en su formación, se han venido celebrando una serie de reuniones en diversas capitales del mundo (la mas reciente tuvo lugar El Cairo los días 7-10 de Marzo).

A todo esto NSI ha tratado por todos los medios de impedir la constitución de ICANN. Ello hasta el punto de no reconocer su autoridad e incluso hizo cambios en su gestión de nombres que en un momento dado pusieron en peligro la estabilidad de Internet. Entre sus varias acciones obstaculizantes, citamos el caso del establecimiento de nuevas entidades de registro de nombres. A lo largo de 1999 , y en consonancia con los acuerdos derivados del "White Paper", NSI debía permitir que otras entidades pudiesen tambien registrar nombres.

A tal fin en una fase inicial de pruebas, que finalizó en junio, paticiparon 5 empresas. A partir de ahí se autorizó el resto de las otras empresas solicitantes (Registrars). Entre ellas la española/catalana, Nominalia. NSI debería, no solo permitir, sino que ademas debería facilitar la entrada de los nuevos Registrars, sin embargo hizo todo lo contrario a través de una serie de impedimentos.

En medio de esta situación, en fechas previas a la reunión de Los Angeles (1- 4 de noviembre, 1999), las conversaciones entre ICANN, NSI y el gobierno USA habían conducido a una serie de acuerdos preliminares. Estos acuerdos, antes de su aprobación por ICANN se pusieron sobre la Red, para el comentario público (una vez mas desde Galicia hemos enviado NUESTRA OPINION al respecto). Los comentarios recibidos desde todo el mundo fueron analizados por ICANN y finalmente el 10 de noviembre se firmaban los nuevos acuerdos entre ICANN, NSI, y el gobierno USA.

En algunos puntos y como consecuencia de los comentarios globales, los acuerdos fueron modificados. En otras palabras, NSI se doblegó y se ha vuelto un tanto mas dócil, pero... aun mantiene control de los "root servers" y la gestion de la base de datos de los dominios ".com", ".org" y ".net", sobre el DNS correspondiente (dicha base de datos se conoce bajo el nombre conocida como "registry database"). En su día, dicho control pasará a ser ejercido por ICANN pero, de momento, su entrega a la nueva entidad todavía depende del gobierno USA.

La realidad actual es que de forma, quizás lenta, pero firme ICANN sigue su evolución hacia su constitución como la entidad internacional independiente que gobernará Internet.

La membresía Global de ICANN

Como se mencionó antes, la estructura de su gobierno (de ICANN), estará formada por 18 Directores y un Presidente. De esos 18 Directores, ya han sido elegidos los 9 relacionados Organizaciones de Apoyo (Nombres de DNS, Numeros IP y el Protocolo TCP/IP). Todos los elegidos son individuos de relevancia en Internet. Entre ellos están Vint Cerf (creador del protocolo y conocido como "padre de Intenet"9 y un un español Amdeu Abril (en el area de nombres).

Quedan por elegir los 9 restantes y hasta cierto punto los mas IMPORTANTES. Se trata de los 9 DIRECTORES GLOBALES (conocidos como Directors At-Large). La importancia de estos 9 directores es que serán los REPRESENTANTES DE LA COMUNIDAD INTERNETICA GLOBAL en esta entidad de gestión. ¿Como conseguir que esas 9 personas elegidas, representen a la comunidad de internautas global? ¿Como elegirles? ¿Quien les elige? ¿Que cualidades deben reunir los candidatos a dichos puestos?.

Estos se encargarán de la formación de dicha membresía en sus paises respectivos y asimismo nombrar coordinadores en los restantes paises europeos. Actualmente, cualquier internauta puede hacerse miembro del ICANN si cumple los siguientes requisitos:

1) Ser mayor de edad (de acuerdo a las leyes del pais donde vive)
2) Disponer de una dirección de correo electrónico.
3) Disponer de dirección postal y poder demostrar (caso se le pidiese) que es residente/ciudadano del pais donde dice que vive.

2. Evolución de la ICANN

Las reformas de la ICANN desde un punto de vista crítico

ICANN nos quiere quitar Internet de las manos
por Melisa Tuya
01/07/2002, 17:17 GMT+1
Disponible en
http://www.baquia.com/com/20020701/art00010.html

Una versión remozada hace un par de semanas de la controvertida propuesta que Stuart Lynn presentó en febrero y que aboga porque los internautas vean aún más mermada su presencia en esta corporación en beneficio de un mayor control gubernamental de Internet, ha sido aprobada por unanimidad (con la ausencia de Karl Auerbach, internauta de a pie elegido por los estadounidenses) por el Consejo de Dirección de la ICANN (Internet Corporation for Assigned Names and Numbers).

Más concretamente, lo que se ha decidido en Bucarest es no permitir que los internautas corrientes y molientes puedan pertenecer al Consejo de esta organización con sede en California. Hasta el momento cinco de los 19 directivos de la ICANN eran

simples navegantes, elegidos mediante una votación en la que cualquier internauta que lo deseara podía participar.

A partir de ahora el control de los servidores raíz, los protocolos de Internet y el sistema de nombres de dominio estará en manos únicamente de organizaciones técnicas, empresas, gobiernos y entidades sin ánimo de lucro. Vamos, que la democracia está muy bien, pero según para qué cosas.

También se han apuntado otro tipo de novedades, como empezar a cobrar unos 25 centavos por cada nuevo dominio registrado para poder financiarse de mejor manera. Algo que muchos que ya han tachado como una "tributación sin representación". Un impuesto que no va a satisfacer demasiado a Verisign, la empresa estadounidense que gestiona los principales dominios de alto nivel (y por tanto se lucra con cada nueva entrada), y que desde hace tiempo mantiene unas relaciones bastante tirantes con la ICANN.

No obstante, para cerrar las puertas de la ICANN en las narices de los internautas de manera definitiva, aún queda obtener el visto bueno del Consejo en la próxima reunión que tendrá lugar en China durante el mes de octubre. Algo que parece ser cosa hecha. Mientras llega ese momento, un comité estudiará detenidamente la propuesta, incluyendo modificaciones si lo considera conveniente.

Entre la espada y tres paredes

Otorgar más poder a los gobiernos era algo que ha acabado siendo inevitable, dada la presión ejercida en este sentido desde todos los puntos cardinales a lo largo de las últimas semanas.

Primero fue Stuart Lynn quien dijo que quería que los gobiernos participasen más en la gestión de la corporación que preside. Su teoría era que encontrar mediante una votación mundial un puñado de representantes adecuados para más de 425 millones de internautas es prácticamente imposible, mientras que los gobiernos representarán adecuadamente los intereses de sus ciudadanos, ya que les han elegido democráticamente.

Además, Lynn reconocía que la ICANN necesitaba una reforma como el comer, y que "si una cosa ha quedado clara durante los últimos tres años es que una entidad puramente privada que depende de la cooperación voluntaria de muchas otras entidades no es capaz de coordinar nada globalmente sin un apoyo gubernamental". La presión desde dentro estaba servida.

Luego, tanto el gobierno estadounidense como la Unión Europea dejaron bien claro su deseo de meter aún más la cuchara en el pastel de la gestión de Internet. El primero está revisando la 'carta otorgada' mediante la cual cedió a la ICANN sus potestades y clamando por una mayor transparencia de la organización si no quiere que le recorte sus poderes (y aquí no valdría rezar a Santa Rita).

De todas maneras, la ITAA (Information Technology Association of America) ya ha adelantó que creía que el Departamento de Comercio y la ICANN renovarían de nuevo su contrato (que se lleva prolongando desde 2000, fecha en la que la ICANN podría haber cedido su control sobre los nombres de dominio a otra empresa u organización). Probablemente a día de hoy esta asociación que defiende los intereses del sector privado esté aún más segura de ello.

En cuanto a la vieja Europa, su Consejo de Telecomunicaciones se dedicó a discutir en Luxemburgo durante el mes pasado si representaba de manera adecuada los intereses públicos, llegando a la conclusión de que el Comité Asesor Gubernamental

(GAC por sus siglas en inglés) debería tener más poder dentro de la ICANN, teniéndose siempre en cuenta su opinión antes de tomar una decisión e incorporando sus recomendaciones en la resolución.

Anna Birulés ministra española de Ciencia y Tecnología y presidenta del Consejo de Telecomunicaciones, defendió que los gobiernos tienen derecho a definir los principios que deben respetarse para mejorar la representación y defensa de los intereses generales en asuntos relacionados con la gestión internacional de Internet.

De poco parece que pueda servir

De sobra es sabido que la ICANN, pese a su juventud (nació en 1998 por obra y gracia del gobierno Clinton), necesitaba una reforma con urgencia. También es cierto que uno de sus principales problemas, que arrastra desde su misma concepción, es el de la falta de legitimidad (otros son su ineficacia y su inclinación por favorecer los intereses de los Estados Unidos). Lo que no parece tan claro es que apartar a los internautas aún más de lo que ya estaban vaya a solventar lo más mínimo estas cuestiones.

ICANN es una casa con los cimientos temblorosos, su problemática es profunda y complicada, y esta medida puede incluso agravar esa situación por mucho que agrade a los progubernamentales. De hecho, desde que se hizo pública esta reforma a finales de la pasada semana, los diferentes colectivos e individuos críticos con esta corporación (que son legión, y será por algo) no han cesado de llover.

También en Bucarest

También en su esperada reunión rumana, poco antes de aprobar esta polémica propuesta, la ICANN anunció dos medidas para acabar con los especuladores de dominios. Una especie que, aunque ya no haga tanto ruido, aún está lejos de encontrarse en peligro de extinción.

Por una parte, y para evitar que los dominios que empresas o instituciones olvidan renovar caigan en manos de gente poco escrupulosa, pretende conceder a los propietarios de dominios un tiempo extra para renovar sus contratos (30 días). Esta propuesta tuvo una buena acogida.

Por otro lado quiere establecer listas de espera para los nuevos dominios jugosos que vayan llegando. Algo más complicado de conseguir. La solución sugerida por Verisign no parece que fuera a beneficiarle más que a ellos, al querer cobrar una cuota de 28 dólares para estar entre los que tienen más opciones de hacerse con nuevos dominios.

http://www.baquia.com /com/20021031/not00011.html

Baquía > La Red > Noticia 17 feb 2003

La ICANN elimina las elecciones directas
por Redacción de Baquía
04/11/2002, 09:58 GMT+1

La ICANN, máximo y discutido organismo gestor de Internet, ha acabado haciendo algo que venía amenazando desde hace algún tiempo: ha votado en China a favor (15 a 3) de eliminar las elecciones directas. Una medida que se enmarca dentro de las apuntadas hace tiempo por su presidente Stuart Lynn para mejorar la eficacia de la

organización, pero que según los críticos evitará que los navegantes ordinarios participen.

Según el nuevo sistema aprobado, el consejo será elegido por un comité designado a tal efecto y un trío de organizaciones afiliadas que representen los grupos de poseedores de direcciones. Los cambios tendrán lugar en la conferencia de la ICANN que está prevista para diciembre en Amsterdam.

Mary Hewitt, portavoz de la ICANN, ha asegurado al respecto que "cada sector, desde los grupos no comerciales hasta los empresariales, han expresado su apoyo por este proceso de reforma. Un montón de dialogo constructivo está teniendo lugar, y estamos satisfechos con el progreso por el momento".

Por su parte, Lynn ha asegurado que así se conseguirá que la ICANN "sea una organización mucho más eficiente y efectiva que podrá conseguir cosas mucho mejor y más rápidamente y que estará más conectada ala comunidad de lo que lo está ahora".

Aunque no todo el mundo, ni mucho menos, se muestra tan conforme con una decisión que otorga mas poder a los gobiernos y resta credibilidad a este organismo. Incluso dentro de la ICANN florecen este tipo de planteamientos. Karl Auerbach, uno de sus miembros elegido por los internautas, ha declarado que la "ICANN tiene serios problemas, y este cambio no resuelve ninguno. Quizás los hace peores y los enquista más profundamente en la estructura de la corporación".

Ya en junio del presente año, y también siguiendo la senda marcada por Stuart Lynn, la ICANN decidió que los 19 miembros del consejo de dirección procederían de organizaciones técnicas, empresas, gobiernos y entidades sin ánimo de lucro, pero que en ningún caso podrían presentarse para ocupar ese cargo los internautas de a pie. Entonces, Lynn y los 'progubernamentales' rechazaron toda crítica argumentando que la ICANN estaría formada por políticos y miembros de comunidades que ya han sido elegidos por los internautas.

Con esta nueva decisión, queda de nuevo de manifiesto que el control de Internet tiende cada vez más a escapar de las manos de los internautas, que al fin y al cabo no hacen más que molestar con sus voces disidentes. El mismo Auerbach, ha molestado en numerosas ocasiones. Su afán de saber incluso le llevó a los tribunales para poder acceder a todos los documentos de la organización (algo que intentaba infructuosamente desde 2000).

Evolución ICANN desde 2003

En septiembre y octubre de 2003 la ICANN desempeñó un papel crucial en el conflicto en torno a VeriSign 's "wild card", un servicio de DNS. Después de una carta abierta de la ICANN la expedición de un ultimátum a VeriSign, la empresa voluntariamente acabó el servicio en 4 de octubre de 2003. Tras este paso VeriSign presentó una demanda contra ICANN el 27 de febrero de 2004, alegando que ICANN había sobrepasado su autoridad, buscando a través de la demanda para reducir la ambigüedad sobre la autoridad de ICANN. La lucha contra los monopolios VeriSign componente de la reclamación fue desestimada en agosto de 2004.

El 17 de mayo de 2004, ICANN publicó un proyecto de presupuesto para el año 2004-05. Incluye propuestas para aumentar la transparencia y el profesionalismo de sus operaciones, y aumenta en gran medida su propuesta de gasto. El Consejo Europeo Nacional de dominio de nivel superior Registros (CENTR), que representa los registros de Internet de 39 países, rechazó el aumento, acusando a ICANN de una falta de prudencia financiera. A pesar de las críticas, se llegó a un acuerdo de registro para los dominios de nivel superior .JOBS y .TRAVEL que incluye una tasa de 2 dólares por cada dominio de las empresas autorizadas.

Junto con el éxito de las negociaciones .TRAVEL y .JOBS, los nombres de dominio .MOBI, y .CAT son algunos de los nuevos dominios de nivel superior establecidos por ICANN.

El 10 de mayo de 2006 la ICANN no aprobó un plan para un nuevo ".Xxx" sufijo que han sido designados para los sitios web con contenido pornográfico. ICANN rechazó formalmente .XXX el 30 de marzo de 2007 durante su reunión en Lisboa, Portugal.

El 26 de julio de 2006, el Gobierno de los Estados Unidos renovó el contrato con la ICANN para la ejecución de la IANA por un período adicional de uno a cinco años.

Cuestionario Sobre historia y organización de internet:

Historia

De los pioneros de internet:
Qué aportación hizo a internet

Qué aportación hizo a internet Vannevar Bush

Qué aportación hizo a internet Paul Baran

Qué aportación hizo a internet Douglas Englebart

Qué aportación hizo a internet Vint Cerf

Qué aportación hizo a internet Tim Berners-Lee.

A la vista de los materiales, cuáles eran los cinco requisitos de la respuesta RAND a la pregunta relativa a sistema comunicaciones resistente a ataque nuclear?
1-
2-

3-
4-
5-

A qué responden las iniciales ARPA?

¿Qué finalidad tuvo la primera lista de correo de la historia?

¿Cuándo se generaliza el uso de IP/TCP, cuál era el acrónimo del sistema anterior?

¿Qué aspectos son controlables en internet?

Sobre la organización de la red:

¿Cómo se denominó el periodo conflictivo de 1996?

¿hubo importante participación en las votaciones para los cinco directores "at large" elegidos?

¿Señala tres de los problemas del ICANN en sus primeros años de funcionamiento a juicio de quien fuera su director?

Qué dos hechos destacarías con relación al ICANN desde 2003

Qué críticas se han operado sobre las reformas del ICANN

II. INTERNET Y DERECHO

1. Declaración de Independencia del Ciberspacio, John Perry Barlow.

Fundador de Fronteras Electrónicas. 8 de febrero de 1996

http://www.internautas.org/documentos/decla_inde.htm

Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos.

No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla. Declaro el espacio social global que estamos construyendo independiente por naturaleza de las tiranías que estáis buscando imponernos. No tenéis ningún derecho moral a gobernarnos ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente.

Los gobiernos derivan sus justos poderes del consentimiento de los que son gobernados. No habéis pedido ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas.

No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.

Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis esto como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Donde haya verdaderos conflictos, donde haya errores, los identificaremos y resolvereremos por nuestros propios medios. Estamos creando nuestro propio Contrato Social. Esta autoridad se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente.

El Ciberespacio está formado por transacciones, relaciones, y pensamiento en sí mismo, que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos.

Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento.

Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o el conformismo.

Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia. Aquí no hay materia.

Nuestras identidades no tienen cuerpo, así que, a diferencia de vosotros, no podemos obtener orden por coacción física. Creemos que nuestra autoridad emanará de la moral, de un progresista interés propio, y del bien común. Nuestras identidades pueden distribuirse a través de muchas jurisdicciones. La única ley que todas nuestras culturas reconocerían es la Regla Dorada. Esperamos poder construir nuestras soluciones particulares sobre esa base. Pero no podemos aceptar las soluciones que estáis tratando de imponer.

En Estados Unidos hoy habéis creado una ley, el Acta de Reforma de las Telecomunicaciones, que repudia vuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, DeToqueville y Brandeis. Estos sueños deben renacer ahora en nosotros.

Os atemorizan vuestros propios hijos, ya que ellos son nativos en un mundo donde vosotros siempre seréis inmigrantes. Como les teméis, encomendáis a vuestra burocracia las responsabilidades paternas a las que cobardemente no podéis enfrentaros. En nuestro mundo, todos los sentimientos y expresiones de humanidad, de las más viles a las más angelicales, son parte de un todo único, la conversación global de bits. No podemos separar el aire que asfixia de aquél sobre el que las alas baten.

En China, Alemania, Francia, Rusia, Singapur, Italia y los Estados Unidos estáis intentando rechazar el virus de la libertad erigiendo puestos de guardia en las fronteras del Ciberespacio. Puede que impidan el contagio durante un pequeño tiempo, pero no funcionarán en un mundo que pronto será cubierto por los medios que transmiten bits.

Vuestras cada vez más obsoletas industrias de la información se perpetuarían a sí mismas proponiendo leyes, en América y en cualquier parte, que reclamen su posesión de la palabra por todo el mundo. Estas leyes declararían que las ideas son otro producto industrial, menos noble que el hierro oxidado. En nuestro mundo, sea lo que sea lo que la mente humana pueda crear puede ser reproducido y distribuido infinitamente sin ningún coste. El trasvase global de pensamiento ya no necesita ser realizado por vuestras fábricas.

Estas medidas cada vez más hostiles y colonialistas nos colocan en la misma situación en la que estuvieron aquellos amantes de la libertad y la autodeterminación que tuvieron que luchar contra la autoridad de un poder lejano e ignorante. Debemos declarar nuestros "yos" virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos.

Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes.

Davos, Suiza. 8 de febrero de 1996

2. Las leyes del ciberespacio, de Lawrence Lessig

Las leyes del ciberespacio

Lawrence Lessig

Frente a la idea o mito de libertad total en la red, el artículo es un análisis de las constricciones presentes en la misma. Se plantea la diferencia entre leyes y normas

sociales de cara al uso del ciberespacio, introduciéndose en sus entrelazamientos. Especialmente interesante es el concepto de arquitectura del ciberespacio, que desarrolla más ampliamente en el nº 2 de la misma revista, Cuadernos de Ciberespacio y Sociedad. A partir del mismo, el lector puede empezar a hacerse preguntas, tales como la posibilidad de cambiar las normas sociales en Internet y desde Internet. Además, hay que señalar que el autor se hizo famoso por ser el investigador designado en el caso contra Microsoft.

Cuadernos Ciberespacio y Sociedad Nº 3

Marzo 1999

Traductor: **Javier Villate**

URL del documento original: **cyber.harvard.edu/works/lessig/laws_cyberspace.pdf** (3 abril 1998)
Dispuesto para su acceso en
http://cys.derecho.org/03/leyes.html
http://www.uned.es/ntedu/espanol/master/segundo/modulos/audiencias-y-nuevos-medios/ciberesp.htm

Antes de la revolución, el zar de Rusia tenía un sistema de pasaportes internos. El pueblo odiaba este sistema. Estos pasaportes indicaban de qué estado procedía la persona y esta indicación determinaba los lugares a los que se podía ir, con quién podía uno asociarse, qué podía llegar a ser. Los pasaportes eran distintivos que facilitaban o prohibían el acceso. Controlaban lo que los ciudadanos podían llegar a saber en el estado ruso.

Los bolcheviques prometieron cambiar todo esto. Prometieron abolir los pasaportes internos. Y tan pronto tomaron el poder, lo hicieron. Los rusos volvieron a ser libres de viajar a donde quisieran. Ningún documento que debieran llevar consigo determinaba ya a dónde podían ir. La abolición de los pasaportes internos simbolizó la libertad para el pueblo ruso, una democratización de la ciudadanía en Rusia.

Sin embargo, esta libertad no duraría demasiado. Una década y media después, enfrentados con la perspectiva del hambre, los campesinos invadieron las ciudades en busca de alimento. Stalin reinstauró el sistema de pasaportes internos. Los campesinos volvieron a quedar atados a sus tierras (una restricción que se mantuvo durante la década de 1970). Los rusos se vieron de nuevo restringidos por lo que permitía su pasaporte. Una vez más, para desplazarse por Rusia, los rusos tenían que mostrar algo de lo que ellos eran.

En el mundo real -este mundo, el mundo en el que estoy ahora hablando- la conducta es regulada por cuatro tipos de restricciones. La ley es sólo una de ellas. La

ley regula mediante sanciones impuestas *ex post*: si no pagas tus impuestos, probablemente irás a la cárcel; si robas mi coche, probablemente irás a la cárcel. La ley es la preminencia de los reguladores. Pero sólo es una de las cuatro restricciones.

Las normas sociales constituyen el segundo tipo. Estas también regulan. Las normas sociales -las comprensiones o expectativas acerca de cómo debo comportarme, impuestas no a través de una agencia centralizada, sino mediante las comprensiones o expectativas de casi todos los miembros de una comunidad- dirigen y determinan mi conducta en una variedad de contextos de forma más amplia que cualquier ley. Las normas dicen qué ropa debo vestir, cómo debo sentarme, organizan cómo vamos a interactuar después de que termine esta charla. Las normas guían la conducta; en este sentido, funcionan como una segunda restricción reguladora.

El mercado es el tercer tipo de restricción. Regula a través del precio. El mercado limita el dinero que puedo gastar en ropa o lo que puedo ganar mediante charlas públicas; dice que puedo exigir por mis escritos menos que Madonna, o menos por mis canciones que Pavarotti. Mediante el precio, el mercado asigna mis opciones y a través de estas, regula mi conducta.

Y, finalmente, tenemos la restricción de lo que podríamos llamar naturaleza, pero que prefiero denominar "arquitectura". Esta es la restricción que presenta el mundo tal y como lo encuentro, aunque sea un mundo que otros han hecho antes. El hecho de que no pueda ver a través de esa pared es una restricción de mi capacidad para saber qué está sucediendo al otro lado de la misma. El hecho de que no haya una rampa de acceso a una biblioteca restringe la entrada de quien debe utilizar una silla de ruedas. Estas restricciones regulan, en el sentido que doy aquí a ese término.

Para entender una *regulación,* tenemos que comprender la suma y combinación de estos cuatro tipos de restricciones. Ninguno de ellos por sí solo puede representar el efecto de los cuatro juntos.

Esta es la era de lo ciber-libertario. Vivimos en un momento en el que se ha hecho muy popular cierta imagen falsa del ciberespacio. Esta es más o menos la siguiente: el ciberespacio es inevitable, más aún, es irregulable. Ninguna nación puede vivir sin él, más aún, ninguna podrá controlar la conducta de las personas en él. El ciberespacio es ese lugar en el que los individuos están, inherentemente, libres del control de los poderes soberanos del espacio real.

Mi punto de vista sobre el ciberespacio es diferente. Mi objetivo es criticar esta imagen falsa. En mi opinión, el mundo en el que estamos entrando no es un mundo de libertad perpetua; o más precisamente, el mundo en que estamos entrando no es un mundo en el que la libertad esté asegurada. El ciberespacio tiene el potencial de ser el espacio más plena y extensamente regulado que hayamos conocido jamás en cualquier lugar y en cualquier momento de nuestra historia. Tiene el potencial de ser la antítesis de un espacio de libertad. Y, a menos que comprendamos este potencial, a menos que

veamos cómo podría desarrollarse, es probable que no nos enteremos de esta transición de la libertad al control. Y, en mi opinión, esa es la transición que estamos viendo precisamente ahora.

Quiero aclarar esto utilizando las dos introducciones con las que he empezado hoy: el relato sobre la Rusia bolchevique y la idea de la regulación. Las dos juntas nos ayudarán a ver a dónde va el ciberespacio y, sobre todo, cómo puede evolucionar.

En primer lugar, al igual que en el espacio real, la conducta en el ciberespacio es regulada por cuatro tipo de restricciones. La ley sólo es una de ellas. A pesar de la falsa imagen existente, ya existen leyes en el ciberespacio, las cuales restringen la conducta en el mismo igual que lo hacen en el espacio real.

También hay normas en el ciberespacio, reglas que gobiernan la conducta y exponen a los individuos a las sanciones de los demás. Y también funcionan en el ciberespacio como lo hacen en el espacio real, amenazando con castigos *ex post* impuestos por la comunidad.

Y también sucede lo mismo con el mercado. El mercado constriñe en el ciberespacio como lo hace en el espacio real. Si cambia el precio del acceso al ciberespacio, las restricciones a dicho acceso cambian también. Si cambia la estructura de los precios de acceso, la regulación del acceso marginal se modifica también.

Pero, para nuestros propósitos, la más importante de las cuatro restricciones de la conducta en el ciberespacio es la equivalente a lo que denominé *arquitectura* en el espacio real: lo que llamaré *código*. Por código quiero decir, simplemente, el software y el hardware que constituyen el ciberespacio tal como es: el conjunto de protocolos y reglas implementadas, o codificadas, en el software del ciberespacio mismo, las cuales determinan cómo interactúan, o existen, las personas en este espacio. Este código, al igual que la arquitectura en el espacio real, establece los términos en los que entro, o existo, en el ciberespacio. Y al igual que la arquitectura, no es opcional. No elijo si obedezco las estructuras que establece el código; los *hackers* pueden elegir, pero son casos especiales. Para el resto de nosotros, la vida en el ciberespacio está sometida al código, al igual que la vida en el espacio real está sometida a las arquitecturas del espacio real.

La sustancia de las restricciones del código en el ciberespacio varía. Pero lo que no varía es cómo se experimentan. En algunos lugares, uno debe introducir una contraseña antes de entrar; en otros, uno puede entrar si ha sido identificado. En algunos lugares, las transacciones que uno realiza dejan rastros que permiten relacionarle; en otros lugares, esta relación es establecida sólo si el individuo lo elige así. En algunos lugares, uno puede decidir hablar un lenguaje que sólo el destinatario puede interpretar (mediante el cifrado); en otros lugares, no existe esta opción.

Las diferencias están basadas en el código de estos lugares diferentes. El código, o software, o arquitectura, o protocolos, de estos espacios establece estas características; estas son seleccionadas por los que escriben el código y restringen la

conducta. En este sentido, como la arquitectura en el espacio real, regulan la conducta en el ciberespacio.

El código, el mercado, las normas y la ley, combinados, *regulan* la conducta en el ciberespacio, de la misma forma que la arquitectura, el mercado, las normas y la ley regulan la conducta en el espacio real. Debemos, pues, considerar cómo operan conjuntamente estas cuatro restricciones.

Un ejemplo -un contraste entre una regulación en el espacio real y la misma regulación en el ciberespacio- aclarará este punto. Pensemos en la preocupación (algunos podrán llamarla obsesión) que existe en mi país en torno a la regulación de la indecencia en la red.

Esta preocupación se inició en Estados Unidos a comienzos de 1995. Su origen fue el extraordinario crecimiento de usuarios normales de la red y, por consiguiente, también de usuarios jóvenes, e incluso un crecimiento más extraordinario aún de la disponibilidad de lo que podemos llamar "pornografía" en la red. Un estudio extremadamente polémico (y básicamente defectuoso), publicado por la revista de derecho de la Universidad de Georgetown, decía que la red estaba inundada de pornografía. *Time* y *Newsweek* trataron el tema. Y los senadores y congresistas fueron bombardeados con demandas de hacer algo para regular la "ciberporquería".

Se desató la furia. Pero podemos preguntarnos por qué fue tan grande esta furia sobre la pornografía en el ciberespacio. A decir verdad, existe más pornografía en el espacio real que en el ciberespacio. ¿Por qué tanta furia ante la pornografía en un lugar al que la mayoría de los chicos no tienen acceso?

Para responder a esa pregunta, pensemos por un segundo en cómo se plantea el mismo problema en el espacio real. ¿Qué regula la distribución de pornografía en el espacio real?

En primer lugar, en Estados Unidos, las leyes en el espacio real regulan la distribución de pornografía entre los adolescentes. Son leyes que exigen a los vendedores de pornografía que comprueben la edad de los compradores, o leyes que exigen que los vendedores se ubiquen en una zona de la ciudad fuera del alcance de los chicos. Pero las leyes no son las restricciones más importantes en la distribución de pornografía entre los chicos.

Más importantes que las leyes son las normas. Las normas dificultan que los adultos vendan pornografía a los adolescentes. Esta restricción es incluso relativamente efectiva entre los distribuidores de pornografía.

Pero no sólo las normas sociales intervienen. También lo hace el mercado, con los precios de la pornografía que los chicos no pueden pagar.

Pero la restricción más importante en el espacio real es lo que he llamado *arquitectura*. Todas las demás limitaciones dependen de esta. Las leyes, las normas y

el mercado pueden discriminar el acceso de los adolescentes en el espacio real, porque es difícil ocultar que eres un menor. Por supuesto, un chico puede ponerse un bigote y unos zancos y entrar en una tienda porno para comprar pornografía. Pero normalmente, no lo conseguirá. Para la mayoría será bastante difícil ocultar su edad. Por eso, generalmente, las restricciones basadas en la edad pueden ser efectivas.

El ciberespacio es diferente. Incluso si asumimos que las mismas leyes del espacio real se aplican al ciberespacio y que las restricciones de las normas y del mercado también tienen lugar, sigue habiendo una diferencia básica entre los dos espacios. Porque mientras que en el espacio real es difícil ocultar que tú eres un menor, en el ciberespacio ocultar quién eres o, más exactamente, tus características identificadoras es la cosa más sencilla del mundo. La condición predeterminada en el ciberespacio es la anonimidad. Y al ser tan fácil ocultar quién es uno, es prácticamente imposible que las leyes y las normas se apliquen en el ciberespacio. Para que estas leyes se apliquen, uno tiene que saber que la persona con la que está tratando es un menor. Pero la arquitectura del ciberespacio, simplemente, no ofrece esa información.

Ahora lo que importa es ver la diferencia e identificar su origen. La diferencia está en lo que denominaré *regulabilidad* del ciberespacio, es decir, la capacidad de los gobiernos de regular la conducta en el ciberespacio. Tal y como lo conocemos ahora, el ciberespacio es un espacio menos *regulable* que el espacio real. El gobierno, aquí, puede hacer poca cosa.

El origen de esta diferencia de regulabilidad está en la arquitectura del ciberespacio: en el código que constituye el ciberespacio tal como es. Su arquitectura, en mi opinión, es esencialmente irregulable.

O, por lo menos, lo era en 1995 y en 1996, cuando el Congreso de Estados Unidos intentó sacar adelante la Ley de Decencia de las Comunicaciones. Voy a hablar un poco sobre lo que pasó con esta ley, pero primero quiero destacar este periodo y ver dónde estamos hoy. Fue la arquitectura del ciberespacio en 1995 y 1996 lo que lo hacía esencialmente irregulable.

Llamemos a esa arquitectura *Red 95* -ya que se refiere a 1995- y veamos cuáles eran sus características. Si uno tenía acceso a *Red 95*, podía pasearse sin revelar su identidad. *Red 95* era como la Rusia bolchevique. La propia identidad o características personales eran invisibles para los demás en esos tiempos y uno podía entrar y explorar sin presentar ningún tipo de credencial, sin un pasaporte interno. El acceso era abierto y universal, no estaba condicionado a la presentación de credenciales. Era, en el sentido estricto del término, un momento extraordinariamente democrático. Los usuarios eran fundamentalmente iguales. Esencialmente libres.

Fue en este contexto, *Red 95*, que la Corte Suprema enjuició la Ley de Decencia de las Comunicaciones. Dos tribunales de rango inferior habían anulado la ley por considerarla una violación del derecho a la libertad de expresión. Millones de personas siguieron el juicio y los argumentos que en el mismo se expusieron.

En junio del año pasado, la Corte confirmó las decisiones de los tribunales de rango inferior y declaró que la ley era inconstitucional. No nos interesa ahora examinar por qué era inconstitucional. Lo importante, para nuestros propósitos, es la retórica que llevó a la Corte a tomar esa decisión.

La decisión dependía, de forma crucial, de las concepciones sobre la arquitectura de la red de entonces, es decir, de *Red 95*. Dada esa arquitectura, la Corte concluyó que cualquier regulación que intentara zonificar el acceso de los menores a la pornografía sería excesivamente gravosa para los emisores y receptores. Tal y como era la red entonces, la regulación sería demasiado gravosa.

Pero lo importante fue que la Corte habló como si esta arquitectura de la red -*Red 95*- fuera la única arquitectura posible de la red. Habló como si hubiera descubierto la naturaleza de la red y, por consiguiente, estaba decidiendo la naturaleza de cualquier posible regulación de la red.

Pero el problema es que, evidentemente, la red no tiene naturaleza alguna. No hay una única arquitectura que sea esencial en el diseño de la red. *Red 95* es un conjunto de características o protocolos que constituían la red en un periodo determinado de tiempo. Pero nada exige que estas características o protocolos hayan de constituir para siempre la red. Y, de hecho, nada de lo que hemos visto en los dos últimos años puede llevarnos a pensar que vaya a ser así.

Un ejemplo puede aclarar este punto. Antes de que fuera profesor de Harvard, enseñé en la Universidad de Chicago. Si uno quería acceder a la red en esta universidad, sólo tenía que conectar su ordenador a los enchufes que había por toda la universidad. Cualquier ordenador podía conectarse a esos enchufes y, una vez conectado, cualquier ordenador podía tener pleno acceso a Internet. El acceso era anónimo, completo y libre.

La razón de que existiera esta libertad fue una decisión de la administración. El director de la Universidad de Chicago es Geof Stone, ex decano de la Facultad de Derecho de la Universidad de Chicago y un prominente experto en libertad de expresión. Cuando la universidad diseñó su red, los técnicos le preguntaron si iba a permitir las comunicaciones anónimas. El director, citando el principio de que las reglas que regulen la libre expresión en la universidad debían ser tan protectoras de la libertad de expresión como la Primera Enmienda, dijo que sí: cualquiera podía tener el derecho a comunicar anónimamente en la universidad, puesto que la Primera Enmienda de la Constitución garantizaba ese mismo derecho frente al gobierno. El diseño de la arquitectura de la red de la Universidad de Chicago se derivó de esa decisión política.

En Harvard las reglas son diferentes. Uno no puede conectar su ordenador a la red de Harvard, a menos que dicho ordenador esté registrado, autorizado, aprobado, verificado. Solamente los miembros de la comunidad universitaria pueden registrar sus ordenadores. Una vez registrado, todas las interacciones con la red son potencialmente supervisadas y asignadas a un ordenador determinado. En realidad, la comunicación anónima no está permitida en esta red. El acceso puede ser controlado en base a la

identidad de cada cual y las interacciones pueden ser supervisadas, en base a lo que cada cual hizo.

La razón de este diseño se debe también a una decisión de un administrador; aunque, en esta ocasión, se trate de un administrador menos interesado en las protecciones de la Primera Enmienda. En Harvard, el ideal es controlar el acceso; en Chicago, el ideal era facilitar el acceso. Por tanto, en Harvard se eligieron las tecnologías que hacían posible el control; en Chicago se eligió las tecnologías que facilitaban el acceso.

Esta diferencia entre las dos redes se ha hecho bastante común en nuestros días. La red de la Universidad de Chicago representa la arquitectura de Internet en 1995. Es, una vez más, *Red 95*. Pero la arquitectura de Harvard no es una arquitectura de Internet. Es, más bien, una arquitectura de *intranet*. La diferencia es esta: dentro de una *intranet*, la identidad está lo bastante establecida como para que el acceso pueda ser controlado y el uso, supervisado. Los protocolos subyacentes son todavía TCP/IP, es decir, los protocolos fundamentales o subyacentes de Internet. Pero superpuesto a los mismos hay un conjunto de protocolos que facilitan el control. La red de Harvard es Internet *plus*, donde el *plus* significa poder de control.

Estas dos arquitecturas reflejan dos filosofías distintas sobre el acceso. Reflejan dos conjuntos de principios, o valores, sobre cómo deben controlarse los contenidos. En mi opinión, reflejan la diferencia entre regímenes políticos de libertad y regímenes políticos de control. Reflejan la diferencia ideológica entre la Alemania del Oeste y la del Este; entre los Estados Unidos y la antigua Unión Soviética; entre la República China y la China continental. Es una diferencia entre la libertad y el control, la cual se expresa en la arquitectura o el diseño del código. Estas arquitecturas posibilitan valores políticos. Son, en ese sentido, políticas.

No trato con ello de criticar a Harvard. Harvard es una institución privada; es libre, en una sociedad libre, de asignar sus recursos como desee. Lo que pretendo es hacer ver cómo hay muchas arquitecturas y, por tanto, cómo elegir una u otra es una opción política. Y cómo, a nivel nacional, la arquitectura es inherentemente política. En el mundo del ciberespacio, la elección de una arquitectura es tan importante como la elección de una constitución. Básicamente, el código del ciberespacio *es* su constitución. Establece los términos en los que la gente accede al mismo; establece las reglas, controla nuestras conductas. En este sentido, es su verdadero poder soberano. Un poder soberano alternativo, que compite con los poderes soberanos del espacio real en la regulación de la conducta llevada a cabo por los ciudadanos del espacio real.

Pero la Corte Suprema de los Estados Unidos trató la cuestión de la arquitectura como si la misma fuera algo dado. Habló como si sólo existiera un único diseño posible para el ciberespacio: el diseño que, de hecho, tenía.

En esto, la Corte Suprema no está sola. En mi opinión, el mayor error de los teóricos del ciberespacio -de los ideólogos y, especialmente, de los abogados que piensan en la regulación de este espacio- es el mismo que el de la Corte Suprema. Es el

error del naturalismo aplicado al ciberespacio. Es el error de pensar que la arquitectura que tenemos ahora será la que tendremos siempre; que el espacio nos garantizará la libertad; que nos librará de los gobiernos que quieren controlarnos.

Este punto de vista es profundamente erróneo. Lo es porque, mientras celebramos la libertad "inherente" de la red, la arquitectura de la red está cambiando ante nosotros. La arquitectura está pasando de ser una arquitectura de libertad a una de control. Está cambiando ya sin la intervención del gobierno, aunque este está examinando rápidamente cómo podría intervenir para acelerar ese cambio. Y donde el gobierno está interveniendo, lo está haciendo en una forma pensada para cambiar precisamente esta arquitectura, para convertirla en una arquitectura de control, para que sea, como he dicho, más *regulable*. Mientras los ideólogos prometen una libertad eterna incorporada en la misma arquitectura de la red, técnicos y políticos están trabajando juntos para cambiar esa arquitectura, para desmantelar esta arquitectura de libertad.

Como teóricos de este espacio, debemos comprender este cambio. Debemos reconocer las consecuencias políticas de este cambio. Y debemos responsabilizarnos de estas consecuencias. La trayectoria del cambio es inconfundible y el fruto de esta trayectoria, veneno.

Como constitucionalistas, debemos afrontar una cuestión fundamentalmente constitucional: si tenemos la opción de elegir entre arquitecturas de control y arquitecturas de libertad, ¿cómo decidimos estas cuestiones constitucionales? Si las arquitecturas son muchas, ¿nos guiará la misma constitución en la selección de tales arquitecturas?

En mi opinión, los valores constitucionales implican la arquitectura de este espacio. En mi opinión, los valores constitucionales deberían guiarnos en nuestro diseño de este espacio. Y, en mi opinión, los valores constitucionales deberían limitar los tipos de regulabilidad que esta arquitectura permite.

Pero mi punto de vista está ausente de la reflexión actual sobre el papel del gobierno en el ciberespacio. En realidad, mi país -durante muchos años símbolo de libertad en un mundo en el que esta escaseaba- se ha convertido en líder en favor de este cambio de una arquitectura de libertad en Internet hacia una arquitectura de control; de una arquitectura que abrace las tradiciones de libertad expresadas en nuestro pasado constitucional, a una arquitectura que es fundamentalmente contraria a esas tradiciones.

¿Pero cómo puede el gobierno hacer estos cambios? ¿Cómo podría el gobierno imponer este control? Muchos no son capaces de ver cómo el gobierno puede imponer este control. En los pocos minutos que me restan, intentaré mostrarlo. Quiero insistir en el camino que va desde donde estamos en la actualidad hasta donde me temo que nos estamos dirigiendo. Quiero que vean cómo estos cambios son posibles y cómo el gobierno puede ayudar a que sean permanentes.

Volvamos, pues, a la idea con la que empecé este ensayo -la cuestión sobre las diferentes modalidades de restricción- y señalemos algo importante sobre esa idea que hemos remarcado hace poco. Dije al principio que debíamos pensar en la ley como una más de las modalidades de restricción; que debíamos pensar en ella como una parte de la estructura de contención que regula nuestras conductas.

Alguien podría tomar eso como un argumento sobre la insignificancia de la ley. Si hay otras muchas fuerzas, además de la ley, que también regulan, eso podría significar que la ley, por sí sola, puede hacer bien poco.

Pero señalemos algo que debería ser obvio. En el modelo que he descrito, la ley regula mediante una regulación directa -regulando la conducta individual a través de la amenaza de castigo. Pero la ley también regula de otras formas. Lo hace tanto directa como indirectamente. Y lo hace indirectamente cuando regula estas otras modalidades de restricción, con el fin de que regulen de forma diferente. Es decir, puede regular las normas para que estas, a su vez, regulen de forma diferente; y puede regular la arquitectura para que esta, a su vez, regule de forma diferente. En cada caso, el gobierno puede cooptar las otras estructuras, de forma que restrinjan los fines del gobierno.

Este tipo de regulación indirecta es también posible en el ciberespacio. Pero aquí esta regulación indirecta puede ser incluso más importante. Aquí el gobierno no puede regular sólo indirectamente para hacer avanzar un fin sustantivo particular del gobierno. Más importante aún, el gobierno puede regular para cambiar la misma *regulabilidad* del espacio. Es decir, el gobierno puede regular las arquitecturas del ciberespacio de forma que la conducta en el mismo sea más regulable, pues se trata de una arquitectura potencialmente más regulable que ninguna otra que hayamos conocido en la historia del gobierno moderno.

Dos ejemplos aclararán esto. Uno se refiere a la regulación gubernamental de un fin sustantivo particular, y el otro, derivado del primero, es un ejemplo de regulación gubernamental para incrementar la regulabilidad.

El primero es la regulación de la criptografía. El interés del gobierno en la criptografía tiene que ver con el uso de esta tecnología para proteger la privacidad; su capacidad para ocultar el contenido de las comunicaciones a los ojos de una tercera parte vigilante, sea esta el mismo gobierno o un vecino curioso. Durante buena parte de la historia de esta tecnología, el gobierno norteamericano la ha regulado intensamente; durante un tiempo amenazó con prohibir su uso, ha prohibido insistentemente su exportación (como si sólo los norteamericanos entendieran las matemáticas de alto nivel) y ha intentado que el mercado se viera invadido con tecnologías de cifrado estándar que incorporaran una "puerta trasera" para que el gobierno interceptara las comunicaciones.

Las propuestas más recientes son las más importantes. En noviembre pasado, el FBI propuso una ley que exigiría a los fabricantes que garantizaran que cualquier sistema de cifrado que desarrollaran incluyera la posibilidad de recuperar, obtener, las

claves de cifrado o una "puerta trasera" equivalente, de forma que los agentes del gobierno pudieran, si lo necesitaban, acceder al contenido de las comunicaciones.

Esta es una regulación gubernamental del código que regularía indirectamente las conductas. Es indirecta en el sentido que he descrito anteriormente y, desde una perspectiva constitucional, es brillante. No porque su fin sea bueno, sino porque la constitución norteamericana, por lo menos, ofrece muy poco control sobre una regulación gubernamental como esta. La constitución norteamericana ofrece pocas protecciones contra la regulación gubernamental de las empresas y, dado los intereses de estas, es probable que las regulaciones de este tipo sean efectivas.

Mi segundo ejemplo se deriva del anterior. Una segunda utilización de la criptografía es la identificación: de la misma forma que se oculta lo que alguien dice, mediante certificados digitales puede utilizarse para autentificar quién dice algo. Con la capacidad de autentificar quién es quién, el gobierno podría decir de dónde viene alguien o qué edad tiene. Y con esta capacidad -mediante sistemas de identificación o pasaportes para las superautopistas de la información- los gobiernos podrían regular mucho más fácilmente la conducta en el ciberespacio. Esto recrearía el poder de controlar la conducta, recrearía el poder de regular.

Reparemos en lo que lograrían estas dos regulaciones. Puesto que Estados Unidos es el mercado más grande de productos de Internet, ningún producto puede esperar tener éxito a menos que lo tenga en los Estados Unidos. Así, los estándares impuestos con éxito en Estados Unidos se convierten en estándares para el mundo entero. Y, en primer lugar, estos estándares facilitarían la regulación y, en segundo lugar, asegurarían que las comunicaciones de Internet pudieran ser interceptadas por cualquier gobierno que siguiera los procedimientos indicados en la ley. Pero los estándares que esos gobiernos tendrían que cumplir no son los estándares de la constitución de Estados Unidos, sino cualquier estándar que un gobierno local tenga la oportunidad de tener, se trate del gobierno de China continental o de Suiza.

La consecuencia es que el gobierno de Estados Unidos estaría exportando una arquitectura que facilita el control, y no sólo un control ejercido por otros gobiernos democráticos, sino por cualquier gobierno, incluidos los represivos. Por eso, los Estados Unidos dejarían de ser un símbolo de la libertad para convertirse en un vendedor ambulante de control. Tras haber ganado la guerra fría, estaríamos ahora promoviendo las técnicas que nuestros enemigos emplearon durante la guerra fría.

¿Qué debemos hacer? ¿Qué deben hacer ustedes -como poder soberano libre de la influencia de cualquier gobierno extranjero- y nosotros, como constitucionalistas liberales? ¿Qué debemos hacer ante las decisiones de los poderes políticos y económicos dominantes para influenciar la arquitectura mediante la regulación realizada por el código?

Los poderes soberanos deben entender esto. El código del ciberespacio es él mismo una especie de poder soberano. Es un poder soberano competidor. El código es él mismo una fuerza que impone sus propias reglas a la gente que está en el ciberespacio; pero esa gente es también la gente que está aquí, en el espacio real (ciudadanos de la República China, de Francia, de cualquier nación del mundo). El código les regula, aunque sólo estén, por derecho, sujetos a la regulación de sus poderes soberanos locales. El código compite, así, con el poder regulador de los poderes soberanos locales. Compite con las decisiones políticas tomadas por los poderes soberanos locales. Y en esta competencia, a medida que la red se vaya convirtiendo en el lugar dominante de los negocios y la vida social, el código desplazará a las regulaciones de los poderes soberanos locales. Ustedes, como poder soberano, han temido la influencia competidora de otras naciones. Ahora, una nueva nación está enchufada a sus teléfonos y su influencia sobre los ciudadanos es creciente.

Ustedes, como poder soberano, tendrán que reconocer esta competencia. Y tendrán que reconocer y cuestionar el rol especial que los Estados Unidos están jugando en esta competencia. Gracias a la distribución de los recursos que controlan la arquitectura de la red, los Estados Unidos tienen un poder único para influenciar el desarrollo de esa arquitectura. Es como si se estuviera escribiendo la ley de la naturaleza y los Estados Unidos fueran los autores. Este poder da una importante responsabilidad a los Estados Unidos, y ustedes deben asegurarse de que lo ejerce de forma responsable.

Para los constitucionalistas -aquellas personas preocupadas de preservar las libertades sociales y políticas en este nuevo espacio-, el problema es más difícil.

Volvamos al relato con el que inicié esta charla, el mundo de los pasaportes internos. Una forma de entender lo que he dicho hoy sobre el ciberespacio está en la línea de ese relato sobre la Rusia zarista. El nacimiento de la red fue como la revolución; la vida según *Red 95* era como la vida en la Rusia bolchevique (por lo menos, en lo que se refiere a sus partes buenas, como la eliminación de los pasaportes internos); la Red se está convirtiendo en algo parecido a la Rusia estalinista, donde se reinstauraron los pasaportes internos.

Hay una trampa en esta historia, una trampa retórica que tiende a oscurecer un hecho importante sobre la vida en el espacio real. Todos nosotros vivimos en un mundo de pasaportes internos. En los Estados Unidos, en muchos lugares, uno no puede vivir sin un coche, y no puede conducir un coche sin una licencia, y una licencia de conducir es como un pasaporte interno: dice quién eres, de dónde eres, cuántos años tienes, si has estado condenado por un delito recientemente..., vincula tu identidad con una base de datos que revelará si has sido detenido (si has sido condenado o no) o si existe alguna orden de detención contra tí en algún país. La licencia de conducir es el pasaporte interno del moderno estado norteamericano. Y no tengo la menor duda de que su capacidad de control o identificación es mucho mayor que la que existía en la Rusia zarista.

Pero en los Estados Unidos -por lo menos para aquellos que no son inmigrantes o miembros de una minoría marginada- la carga que representan estos pasaportes es liviana. La voluntad de regular, supervisar, rastrear, no es lo bastante fuerte en los Estados Unidos como para apoyar cualquier esfuerzo sistemático dirigido a utilizar estos pasaportes para controlar las conductas. Y esa voluntad no es lo bastante fuerte porque el coste de ese control es muy grande. No hay puestos de control en cada esquina; no se pide a los individuos que se registren cuando se desplazan a otra ciudad; uno puede pasear de forma relativamente anónima la mayor parte del tiempo. Las tecnologías de control son posibles, pero son muy costosas. Y este coste es, en buena parte, la razón de la gran libertad que disfrutamos. Es la ineficiencia de las tecnologías de control en el espacio real lo que produce la libertad en ese espacio.

Pero, ¿qué pasaría si el coste del control descendiera dramáticamente? ¿Qué pasaría si emerge una arquitectura que permitiera una supervisión constante, una arquitectura que facilitara un rastreo continuo de la conducta y del movimiento? ¿Qué pasaría si emergiera una arquitectura que recogiera, sin coste, datos sobre los individuos, su conducta, sobre quiénes quieren llegar a ser? ¿Y qué pasaría si la arquitectura pudiera hacer eso de forma invisible, sin interferir con la vida cotidiana de los individuos en absoluto?

Esta arquitectura es el mundo en que se está convirtiendo la red. Esta es la imagen de un control creciente. Como en el espacio real, tendremos pasaportes en el ciberespacio. Como en el espacio real, estos pasaportes podrán ser utilizados para supervisar nuestra conducta. Pero en el ciberespacio, a diferencia del espacio real, esta supervisión, este rastreo, este control de la conducta será mucho menos caro. Este control se realizará en segundo plano, de forma eficaz e invisible.

No vamos a decir si este cambio es para bien o para mal. En realidad, creo que, como constitucionalistas, debemos reconocer una ambigüedad fundamental en nuestros actuales juicios políticos sobre la libertad y el control. Estamos divididos en las reacciones ante esta imagen de un sistema de control perfecto y, al mismo tiempo, invisible. Muchos dirían que este sistema es maravilloso. Fantástico para atrapar al culpable y con pocas molestias para el inocente. Pero hay muchos, también, que dirían que este sistema es espantoso. Dirían que, mientras profesa nuestros ideales de libertad y no ingerencia del gobierno, habríamos establecido un sistema de control mucho más eficaz que ningún otro en el pasado.

La respuesta a todos estos problemas no es, necesariamente, renunciar a las tecnologías de control. La respuesta no es insistir en que *Red 95* es la arquitectura definitiva de la red. La respuesta es encontrar una forma de *traducir* al diseño de la arquitectura de la red lo que es sobresaliente e importante para nuestras libertades actuales y la democracia constitucional. La cuestión radica en ser crítico con este poder soberano emergente, como lo somos con cualquier otro poder soberano.

¿Cuáles son estos límites? Mientras el gobierno controla e influencia la arquitectura del código de la red, debemos, como mínimo, garantizar que el gobierno no monopoliza estas tecnologías de control. Debemos garantizar que los diferentes

tipos de control que hemos incorporado en la democracia constitucional se incluyen también en la regulación de esta constitución, del código. Debemos garantizar que las restricciones de cualquier democracia constitucional -los límites de la eficacia que constituye la Declaración de Derechos y los sistemas de control y de equilibrios- se incluyen en la regulación del código. Estos límites son los "errores" (*bugs*) del código de una democracia constitucional; y, como dice John Perry Barlow, debemos incorporar estos "errores" en el código del ciberespacio. Debemos incorporarlos de forma que, en base a su ineficacia, podamos recrear algunas de las protecciones que conocemos desde hace tanto tiempo.

El ciberespacio está regulado por leyes, pero no sólo por *la ley*. El código del ciberespacio es una de estas leyes. Debemos examinar cómo este código es un poder soberano emergente -omnipresente, omnipotente, amable, eficaz, creciente- y debemos desarrollar, contra este poder soberano, los límites que hemos desarrollado contra los poderes soberanos del espacio real. Los poderes soberanos dirán siempre -en el espacio real y en el ciberespacio- que los límites y las ineficiencias -los errores- no son necesarios. Pero las cosas cambian demasiado rápidamente como para tener esa confianza. Mi temor no es sólo que no hayamos desarrollado todavía un lenguaje de la libertad contra este poder soberano. Ni que no tengamos tiempo para desarrollarlo. Mi temor es que no tengamos voluntad; esa voluntad de las sociedades libres de las dos centurias pasadas para construir constituciones que protejan la libertad a costa de la eficacia.

3. Entrevistas a J. P. Barlow (2001 y 2004)

Entrevista a Barlow 2001

http://www.ciberpais.elpais.es/d/20010927/cibersoc/s3.htm

Jueves, 27 de septiembre de 2001

Ciberp@ís

JOHN PERRY BARLOW:

"Cuando todo esto acabe Internet en EE UU será una herramienta de vigilancia"

Las autoridades norteamericanas quieren limitar la posibilidad de cifrar mensajes. Los expertos consideran que se trata de una medida inútil para combatir el terrorismo y fatal para la libertad de Internet.

Esteganografía: lo que una imagen esconde

TEXTO: **PEDRO DE ALZAGA**

John Perry Barlow, un estadounidense de 54 años, es el creador de Fundación Fronteras Electrónicas, dedicada a velar por que Internet sea cuanto más libre, mejor. *Ciberp@ís* habló con él gracias al correo electrónico.

Pregunta: ¿Por qué ha comparado la situación de su país con la Alemania nazi?

Respuesta: Porque estamos hablando de un cambio radical en la historia americana de los derechos civiles. No creo que vayamos a tener campos de concentración en EE UU, pero asistimos a lo que probablemente se convierta en el mayor esfuerzo autoritario en la historia de esta república. Aunque parezca un poco excesiva, no está totalmente fuera de tono porque la gente tiene que estar alerta ante un asunto tan grave. Parece que andan a ciegas por una noción general de intimidación que no permite la libertad de expresión, y no porque el Gobierno vaya a arrestarte así como así, sino porque decir algo que pueda considerarse al margen del sentimiento americano puede convertirte en traidor.

P. Pero la mayoría de los ciudadanos está a favor de la limitación del uso de la criptografía. ¿Por qué esta mayoría no percibe ésos riesgos?

R. No sólo no lo ven, sino que tampoco quieren escuchar a nadie que lo denuncie. Sienten que es algo profundamente antipatriótico sugerir siquiera que los autoritarios puedan utilizar esta oportunidad en su propio beneficio. El Congreso ha aprobado un puñado de normas para la regulación de Internet que habían sido rechazadas desde hace años . Nunca he visto una situación tan peligrosa para la libertad en América.

P. Proveedores de Internet han accedido a colaborar con el FBI para pinchar las líneas de sus clientes. ¿Cómo afectará esto cuando desaparezca la amenaza de guerra?

R. Una vez que el FBI instala Carnívoro, nadie lo va a quitar. Y no creo que esto suponga ningún beneficio para las empresas, porque cualquiera que tenga negocios en el ciberespacio, tiene interés en la libertad de expresión. En la economía de la información no hay diferencia entre la libertad de expresión y la libertad de comercio. Cuando todo esto acabe, la Internet de EE UU será una herramienta de vigilancia como nunca quisiéramos haberla visto.

P. ¿Cómo cree que puede afectar esta legislación al resto del mundo?

R. Obviamente, el Gobierno español está profundamente afectado por lo que hace el Gobierno de EE UU. Si prohíbe la criptografía, puede apostar a que el Gobierno español tendrá que prohibirla también, porque hay actualmente una enorme cantidad de energía dedicada a prohibirla globalmente. Cuando el país más poderoso del mundo se está convirtiendo en un Estado policial, ¿qué puede decirse del resto del planeta? EE UU tiene una posición crítica para sentar las bases de los derechos civiles en el mundo.

P. ¿Qué opinión le merece el papel bélico que se atribuye a Internet?

R. Me parece muy desafortunado. Internet supone la posibilidad de que cualquier persona en cualquier sitio pueda expresar cualquier creencia. No me importa si se trata de los talibán, los cristianos o una asociación interplanetaria. Las pequeñas comunidades tiene que tener la posibilidad de expresarse en la red. Usar Internet para otro objetivo [bélico] me parece hacer un mal uso de ella.

P. ¿Cree que la red puede ser un arma más poderosa para quienes intentan limitar las libertades que para quienes las defienden?

R. Internet tiene la curiosa cualidad de ser la más grande herramienta para la liberación y la más grande herramienta para la esclavitud que el mundo haya visto. Por un lado, y usando como ejemplo esta entrevista, un tipo en EE UU manda un mensaje a sus conocidos y un periodista en España lo lee y se pone en contacto con él. Esta posibilidad de que exista una voz global en cada individuo me parece extraordinaria. En el extremo opuesto: el FBI está monitorizando Internet para saber quién está diciendo qué cosa y quién está haciendo tal otra. Cada vez que extiendes esta forma de poder, se abre una nueva forma en que la libertad puede ser violentada.

P. ¿Qué modelo de regulación propone para Internet?

R. Hasta ahora Internet ha sido guiada por gente que tenía muy buenas intenciones. Los internautas han estado a favor de la libertad, pero ahora, en este clima, hay mucha gente dispuesta a abandonar sus derechos con mucha ligereza. Si los internautas no quieren que la red sea libre, no lo será. Estoy bastante seguro de que cuando esto adquiera toda su dimensión la libertad de expresión en la red se verá mermada. He visto a gente derribando sitios *web* críticos con el Gobierno, el cierre de servicios que permiten el anonimato en la red, y al FBI entrando en los proveedores para instalar una máquina con Carnívoro. Así estamos: o nos levantamos por la libertad o vamos a perderla.

P. ¿Qué recomienda para salvaguardar los derechos?

R. Lo más importante es ser valiente. Hablar libremente y sin pensar en el riesgo; demostrar la libertad propia y resistir el impulso de permitir a los terroristas que nos aterroricen. Su objetivo era meternos en una dinámica que hiciera más fácil al Gobierno explotar el espíritu americano. Hay que decirles que pueden derribar un par de edificios, pero no pueden derribar nuestra libertad.

ENTREVISTA A JOHN PERRY BARLOW 2004

http://www.elastico.net/archives/000479.html

FEBRERO 03, 2004

En unos día le vamos a añadir cositas al diseño de Elastico y vamos a empezar a albergar material que está distribuido por otros sitios. Como lo más sencillo para hacerlo es crear una entrada, incluimos aquí algo que ya publicamos hace tiempo en nuestro otro blog. En esta entrevista que le hicimos a John Perry Barlow, cofundador de la EFF y autor de "La economía de las ideas", se dicen unas cuantas cosas necesarias y/o interesantemente polémicas, así que esperamos que la redundancia/obsolescencia no moleste mucho. Uds. sabrán perdonarnos.

JOHN PERRY BARLOW: "DESAFORTUNADAMENTE, LA INDUSTRIA DE LOS CONTENIDOS SE NIEGA A VER LO OBVIO"

Ha criado ganado en un rancho en Wyoming, sido letrista de los míticos Grateful Dead y co-fundado la Electronic Frontier Foundation (Fundación de la Frontera Electrónica). Sus escritos, como el imprescindible "La economía de las ideas", lo han convertido en uno de los innegables gurús de la era digital. Miembro en la actualidad del Centro Berkman para la Sociedad e Internet de la escuela de derecho de la universidad de Harvard, John Perry Barlow participó recientemente allá en un encuentro sobre la extensión e impacto de las nuevas tecnologías en los países en vías de desarrollo. Fue allí donde habló con nosotros sobre la cuestión de la "brecha digital", la actuación de la industria de los contenidos en la era digital, el peligro de los monopolios y la necesidad de defender los derechos del ciudadano en la nueva situación posterior al once de septiembre.

¿Cuáles son los retos que la "brecha digital" presenta, y cuáles son las posibles soluciones?

Nunca he creído realmente en la brecha digital. Como William Gibson dijo, el futuro está aquí, sólo que distribuido irregularmente. No es realmente una cuestión de gente que tiene frente a gente que no tiene, sino de gente que tiene frente a gente que no tiene todavía. Y creo firmemente que aquellos que llegan más tarde puede que vayan más lejos, en virtud de que no tienen los límites impuestos por los hábitos mentales desarrollados durante la era industrial. Por ejemplo, yo diría que aunque la tecnología digital está presente en Alemania bastante pronto, Alemania y Francia y otros países de ese estilo van a quedarse cada vez más atrás en lo que respecta a su capacidad de crear en una economía basada en la información, o de beneficiarse por completo de las

posibilidades que ofrece la tecnología digital [En ese sentido, y apoyando la argumentación de JPB, véase cómo el ?Silicon Valley? alemán es Baviera, una primitiva región agrícola al final de la Segunda Guerra Mundial que no tuvo las rémoras del Rin para saltar de la ?Segunda Ola? a la ?Tercera?. Véase también cómo entre las diez regiones de mayor innovación a nivel mundial se halla el Research Triangle Park entre Raleigh y Durham, parque tecnológico surgido de la nada en la muy tabaquera Carolina del Norte, USA. Finalmente, por dar una nota de obsesión local, ¿alguien se acuerda de aquello de ?Andalucía, la California de Europa?? Quizá la estupidez no estaba en el slogan, sino en quienes fracasaron a la hora de hacerlo realidad]. Mientras que África, donde hasta no hace mucho no había ni un proveedor de Internet entre Ciudad del Cabo y Cairo, ha visto una explosión de conectividad. Recientemente estuve en Acra, Ghana, y había 120 cibercafés. Cualquier sitio al que vas, te encuentras a gente conectándose a Internet y dándole progresivamente un uso económico, entendiendo esta oportunidad mejor que gente que entró en los negocios durante la era industrial [Mi amiga Sarah Guerrero, quien acompañó a JPB en ese viaje, me comentó, no obstante, que la mayoría de los usuarios de los cibercafés se dedicaban a buscar información para abandonar el país. En cuanto a la conectividad, tiene que luchar contra los ladrones que se dedican a tirar postes al suelo para robar el cobre de las líneas de conexión].

Me gustaría mencionar mi propia experiencia en estos temas. Yo crié ganado en un rancho durante la primera mitad de mi vida. No tenía ningún contacto con la industria, ni tenía un trabajo en el sentido tradicional del término. Y fue muy fácil para mí saltarme la era industrial y entrar directamente en la de la información, ya que no tenía ninguna de estos conceptos contra los que luchar y pude ver cosas que otra gente que venía de un contexto industrial tenía problemas para entender. Y hay algunas cosas que tienes que entender completamente para sacarle provecho a la oportunidad digital. Entre ellas, el hecho de que las actividades humanas se organizan según redes planas, redes horizontales de interacción en lugar de las jerarquías industriales. Y si tienes muchos años de jerarquías te cuesta entender cómo funcionan las redes horizontales. Desde un punto de vista agrícola, es como funcionan las cosas y como siempre lo han hecho. La agricultura es horizontal, la industria es jerárquica.

Y es ese tipo de problema de paradigmas lo que le va a facilitar a Latinoamérica el convertirse en un actor relevante en la era digital, a pesar de que pueda parecer que hoy existe una brecha entre Latinoamérica y Norteamérica. También creo que hay grandes ventajas culturales en Latinoamérica. Un deseo común de asociarse en redes, comprensión de cómo las redes funcionan, y realmente la red electrónica es otra capa en la redes social y económica. También hay en Latinoamérica un enorme grupo humano con el mismo idioma, lo cual es muy importante. La Red ha sido predominantemente en inglés, pero espero que en los próximos 30 años el componente de español en la Red, en términos de hablantes, sea tan grande como el inglés.

Así que no me preocupo mucho por la brecha digital, creo que se va a resolver por sí sola. Esto no quiere decir que deba ser ignorada. Dedico gran parte de mi tiempo a viajar por los países pobres tratando de ayudar a la gente a establecer contactos y a

llevarles los resultados de mi propia experiencia, intentando darles el primer empujón. Pero en realidad pienso que es una cuestión de paciencia y de energía.

¿Pero esta energía fluye espontáneamente o debe sobreponerse a una serie de problemas, como los monopolios de los medios de comunicación?

Creo que todos en este planeta tenemos un problema realmente serio, el que la Industria de los contenidos y la Industria de los medios se han integrado de tal manera que las mismas entidades que crean entretenimiento también controlan la infraestructura de las telecomunicaciones. Y tienen un modelo de información basado en los bienes industriales. Creen que no hay ninguna distinción significativa entre una idea y una tostadora, lo cual es una equivocación. Pero pueden imponer esa noción de una forma francamente efectiva en virtud de su propiedad de las propias redes de distribución, a través de las cuales viajan esas mismas ideas. Poseen las redes y creen que poseen las expresiones, los contenidos. Y ahora mismo es esta integración monopolística de la Industria de los medios contra lo que constantemente lucho.

Usted mismo es un artista. ¿Tiene la impresión de que nos estamos moviendo realmente hacia un nuevo paradigma?

Sí. Sin duda. Creo que hemos pensado en la monetization del arte basada casi por completo en esos bienes físicos que les sirven de soporte, como libros, CDs, etc. Como resultado, no comprendimos qué es el arte. Es un verbo, no un nombre. El arte es relación, es algo entre el artista y el público. Y es altamente interactivo, no es algo que deba ser vendido como un producto material, sino como un servicio, como una actuación [?performance?], y su valor no debe estar basado en lo que se ha hecho aplicando valor a lo que no se ha hecho aún, en vez de poner todo su valor en lo que se ha hecho, porque éste es el modelo antiguo. Que no creo que sea una locura, ya que la idea del copyright fue establecer incentivos a la creación. Pero si puedes escribir tres buenas canciones y vivir el resto de tu vida de lo que producen...

Y no sólo tú, sino tu hijo.

Y el hijo de tu hijo, a estas alturas... entonces ¿qué incentivos hay para crear?

Y por tanto, ¿qué piensa que debería hacerse con el copyright y la propiedad intelectual?

Creo que debemos superar la idea de que la expresión intelectual es una propiedad. A menos que estemos hablando de esas expresiones que hayan sido plasmadas en un soporte material [Testigo de vista: En los noventa, no se podían sacar fotos en el Louvre con flash, lo cual tiene sentido, supongo, desde el punto de vista de la conservación; sin embargo, en el 2003 está prohibido el uso de todo tipo de cámaras, sin flash, o de video, en el museo florentino donde se halla en David: incluso sacar fotos con un celular es motivo de reconvención... no es el mármol la propiedad, sino la ?forma? impuesta, expresada en él lo que el museo da por propio]. Yo creo que el copyright tiene futuro, en la medida en la que restrinjamos su aplicación a las propias

copias físicas. Y creo que la solución es deshacernos del copyright en los demás sentidos y establecer formas de contrato que aseguren la financiación de la obra que creas. Me parece que debe haber una cierta dosis de protección legal que asegure que tienes control sobre tus creaciones, de manera que no estés en peligro de que alguien vaya y lo use con propósitos comerciales [Por esas fechas, precisamente, echaba a andar Creative Commons]. Pero creo que hay que superar la idea de que el valor de tu arte va a disminuir porque la gente haga copias sin propósitos comerciales. Tengo una enorme experiencia que me lleva a la conclusión de que la fórmula económica usual que establece que hay una relación directa entre escasez y valor, que es cierta en lo que respecta a bienes físicos, sufre un giro total con respecto a las formas de expresión [idea que explora en su influyente ?The Economy of Ideas?]. Con la expresión, hay una relación directa entre familiaridad y valor. Cuanta más gente haya haciendo copias no comerciales de mis canciones, más gente habrá interesada en mi obra, en acudir a conciertos donde se interprete y, de una forma muy interesante, en comprar el producto comercial.

Y esto ha pasado una y otra vez, pero desafortunadamente la industria de contenidos está tan poseída por la metáfora industrial que se niega a ver lo obvio. Y la industria del cine tiene toda una serie de experiencias que debería indicarles cuál es la dirección a seguir. Jack Valenti consiguió mantener los reproductores de video fuera de este país durante cinco años, porque matarían el negocio. En cuanto la gente pudiera hacer copias de las películas, dejarían de ir a los cines. Pero ya se ve lo que ha ocurrido: hay más gente yendo a los cines que nunca, a pesar de la proliferación de esos videos o, diría yo, precisamente gracias a la proliferación de esos videos. Y la industria del video supone ahora un 70% de los ingresos de la industria del cine. Así que en vez de matar el negocio del cine, fue lo mejor que le pudo pasar nunca. A pesar de esa lección, ahora están intentando parar las copias digitales.

Recuerdo a Jack Valenti en un debate con Lawrence Lessig, diciendo que la Red era lo mejor que le había pasado nunca a la industria del cine, porque le permitía distribuir sus productos a precios justos y razonables.

Ya. Lo que Valenti considera justos y razonable no es lo que cualquier otro considera bueno y razonable. El problema con la industria cinematográfica y musical es que quieren seguir explotando al artista y no están interesados en lo que es justo y razonable, sino en lo injusto e irrazonable. Y tienen los medios para oponerse ya que tienen el único medio de distribución de creatividad intelectual. Pero ahora tenemos otro medio de distribución y tenemos que adaptarnos a él en lugar de continuar con un sistema legal y económico de una era completamente diferente.

Ha mencionado los problemas que plantea este monopolio de los medios y los contenidos. ¿Qué opina del deseo de los gobiernos de extender su control, especialmente después del once de septiembre? Por ejemplo, la nueva potestad que tiene el FBI de investigar a alguien, aunque no esté acusado de nada.

Obviamente estoy muy preocupado por este asunto, como demuestra mi trabajo en la Electronic Frontier Foundation. En la última década hemos intentado promover

medidas que protejan la intimidad y que se opongan a la vigilancia injustificada de los ciudadanos. Y todo esto ha sido borrado sistemáticamente después del once de septiembre. Ahora le es posible al FBI llegar a tu casa sin una orden judicial e instalar un dispositivo entre tu ordenador y el teclado que captura todo lo que tecleas para enviarlo al FBI... sin que sepas siquiera que está ahí. Esto es una seria limitación de la Cuarta Enmienda y, desafortunadamente, el pueblo estadounidense está tan hipnotizado con la alucinación de la amenaza por parte de los medios que está dispuesto a permitirlo todo en este punto para lograr la sensación de que están seguros. Pero no van a sentirse seguros, porque tenemos un gobierno que está haciendo todo lo posible para tener a todo el mundo bajo una permanente sensación de peligro. Esto es, verdaderamente, lo peor que le ha ocurrido jamás al ideal americano. Y eso es ya decir mucho, porque la guerra contra las drogas ya fue algo bien salvaje. Pero esto es aún peor. Y solamente puedo esperar que la gente en el mundo desarrollado recupere la razón y se dé cuenta de que es el peor tipo de derrota el que permitamos a los terroristas que dicten las acciones de nuestros gobiernos, que han estado predispuestos a asegurar la libertad. Espero que esta oscuridad pase [la fecha de la entrevista, recuérdese, es junio del 2002: aún no ha caído ni una bomba sobre Iraq].

Antonio en Entrevistas

4. Entrevista a M. Machado

Santiago Muñoz Machado • Catedrático de Derecho Administrativo de la Complutense]

http://www.elpais.es/c/d/20010118/cibernau/portada.htm

CIBERPAÍS, 18 ENERO 2001

"En Internet se produce la abolición del reino de la ley única"

Tomàs Delclós

P. En una red global, los gobiernos tienen dificultades para ejercer su soberanía. ¿Cómo puede aplicarse el Derecho en Internet?

R. La solución más simple es la universalización. Si una nueva ley ha de regir en el mundo entero, que la dicte una autoridad mundial. La armonización implica que exista una única norma a escala regional o universal. Pero ello es imposible. Los estados no lo permitirían y no es necesario.

P. Usted llega a considerarla peligrosa.

R. Hay problemas técnicos que pueden estar en manos de una autoridad universal (propiedad intelectual, registro de dominios), pero en la mayoría de los casos una autoridad única supone un riesgo para la libertad.

P. Entonces, ¿qué hacer?

R. Hay otras soluciones con más futuro. Por ejemplo, el reconocimiento mutuo de legislaciones que supone reconocer las decisiones judiciales de aquel país y procurar que sea posible la ejecución de la sentencia. Por otra parte, los jueces americanos aplican el "estándar de comunidad local", ya que no existe un estándar global. Por ejemplo, en unos estados está autorizado el juego y en otros no. Si en aquella comunidad está prohibido el juego...,actúan contra su práctica.

P. ¿Y si el servidor está en otro país?

R. Se reprime la conducta en destino y no en origen. Ello, obviamente, supone cortar la comunidad virtual en potencia que supone Internet y fragmentar nuevamente el espacio digital.

P. ¿Y ello es bueno o malo?

R. Inevitable. La soberanía reside en los estados que eventualmente la ceden. Incluso instituciones democráticas universales como la ONU tienen la legitimidad que le prestan los estados que la integran. Siempre será preferible que la ley la administren los estados democráticos que no que las multinacionales la impongan. P. Se predica la necesidad de leyes específicas para la red.

R. Depende de la cultura jurídica de cada país. Los franceses han aprobado 10 veces más leyes sobre la prensa que los anglosajones sin que pueda hablarse de que en un lugar haya más libertad de prensa que en el otro. En el terreno de la criminalidad (pederastia, difamación...) se olvida la virtualidad regulatoria del Código Penal que ya sanciona estas conductas. A veces no se tiene presente que el Derecho no es una técnica o una ciencia que resuelva los problemas sociales. Es un instrumento selectivo que no puede aspirar a solucionar cualquier problema.

P. ¿Cómo se resuelve en el caso de un conflicto entre dos usuarios de Internet de distintos países el decidir qué tribunal de qué país entiende del mismo?

R. Es difícil que los jueces nacionales sean sustituidos por un poder judicial de mayor ámbito. Las instancias judiciales supranacionales tienen unas competencias tasadas estrictamente. El Tribunal de Derechos Humanos de Estrasburgo podría actuar contra la difamación en Internet que no hubiera sido corregida por el juez nacional o contra atentados a la intimidad. El Tribunal de Justicia de la CE podría actuar en determinados ámbitos del comercio electrónico si un Estado pone trabas a la libre circulación de mercancías. Pero salvo en estos supuestos el poder judicial ha de ser de los estados. Otra cosa es que desdeñemos la posibilidad de solucionar conflictos por la vía del arbitraje. En el futuro será importantísimo.

P. En caso de conflicto entre un comprador y un vendedor en línea, una directiva europea ha establecido que el caso se dirima en los tribunales del vendedor. Pero quien tiene que acudir a un tribunal de otro país ha de conocer las leyes de aquel país, aumentan los gastos procesales, etcétera. R. Yo postulo que el damnificado pueda elegir la jurisdicción que le convenga. Hay una importante sentencia en el caso de un ciudadano británico difamado por un diario belga en el que el juez resolvió que podía acudir a la justicia de su propio país para que protegiera su derecho.

P. El juez ha de adquirir conocimientos técnicos.

R. El trabajo básico se hace mediante peritos. La justicia está cada vez más en manos de peritos y es un hecho que pone en peligro la independencia de un juez que ha de pronunciarse sobre un supuesto técnico que desconoce. Habrá que extremar la selección y práctica del peritaje.

P. Usted introduce el concepto de derecho en red.

R. Hay más de una forma de hacer derecho: una es la que Ost ha dicho que es la propia de Júpiter, consiste en producir una ley que emana del poder central y se impone a todos. La revolución jurídica más importante de Internet es que cambiará eso. El lugar donde nace la norma no es único, vamos a un derecho multipolar porque tanto en su creación como aplicación intervienen instancias regionales, estatales, locales e incluso tienen un papel importante entidades privadas que, en Internet, comparten con los gobiernos muchas tareas de ordenación y gobierno. El legislador mismo, en lugar de hacer regulaciones exhaustivas, se ve obligado a reconocer normas de estandarización que impulsan organismos privados no nacionales. Se produce una abolición del reino de la ley única. Las regulaciones más eficaces son las centralizadas, pero en Internet no son aplicables. Esta alternativa es más caótica, menos eficaz, pero favorece el desarrollo de valores como la libertad o la universalización de la cultura. Si esto es a cambio de un poquito menos de orden y poder, no es tan malo.

Cuestionario Sobre introducción al Derecho e internet:

Observa la declaración de Derechos de independencia del ciberespacio.
Haz un resumen de la idea – fuerza de la misma (10 líneas).

Una vez leído el trabajo de Lessig, consideras actual la perspectiva e idea-fuerza de la Declaración de Independencia del Ciberespacio.

Del trabajo de Lessig
Qué tipos de regulaciones afirma el autor que existen

Qué es el "Código" para este autor.

Cuál es la imagen falsa del ciberespacio para el autor

Explica los modelos de código que expone a partir de la experiencia universitaria el autor

Cree el autor que habría de repetirse sentencias como las del Tribunal Supremo de 1996-1997, por qué

Qué papel cree que tiene el gobierno de EEUU en la libertad en la red, cuáles son sus medios para ejercerlo

De las entrevistas a J. P. Barlow:
Qué conexión crees que hay entre el pensamiento de Barlow y Lessig

Qué modelo de regulación propone para la red.

Qué opinión tiene Barlow sobre el problema de la brecha digital.

Cuál es su perspectiva del control de internet tras el 11-s

De la entrevista a Muñoz Machado:
Qué solución cree sobre la regulación de la red. La ve posible?

Qué solución cree posible

Observa su idea de Derecho en red. Expón su concepto e intenta poner un ejemplo a la vista de un sector de regulación.

III. DEMOCRACIA ELECTRÓNICA

De Lorenzo Cotino Hueso, 2010.

1. Terminología, conceptos y concepciones de democracia electrónica

En el primer módulo del curso se hizo clara referencia a la dificultad que implica el tratamiento de democracia como concepto y como concepción. Este mismo problema se reproduce e incluso se acentúa cuando se trata de la llamada "democracia electrónica". De hecho, la variedad y discrepancia parte de la terminología misma.

1. Variada terminología

La terminología en la literatura sobre la materia es muy variada: e-democracia, i-democracia, democracia electrónica, e-participación, participación electrónica, ciberdemocracia, teledemocracia, democratización electrónica, ciberpoder, ciberciudadanía, ciudadanía.com, y un largo etc. A estas formas no dejan de añadirse recientemente otras como e-cognocracia o democracia electrónicamente influida, por ejemplo.

Pese a los intentos por diversos autores de atribuir una connotación particular a estas diferentes terminologías (plasmando diferentes "concepciones" de democracia, en el sentido que se expuso en el módulo 1) lo cierto es que se utilizan unas y otras expresiones casi indistintamente sin consolidarse doctrinalmente.

Por mi parte, prefiero denominar democracia o participación electrónicas, o e-democracia, casi indistintamente, a la concesión de un papel importante a las tecnologías de la información y comunicación (en adelante, TICs) en los procesos democráticos y participativos de los sistemas democráticos liberales. La Recomendación CM / Rec (2009) 1 del Comité de Ministros a los Estados miembros sobre la democracia electrónica (e-democracia), en adelante (Recomendación e-democracia 2009) ha venido a seguir esta noción, al afirmar "como el apoyo y fortalecimiento de la democracia, las instituciones democráticas y los procesos democráticos por medio de las TIC, es sobre todo acerca de la democracia. Su objetivo principal es el soporte electrónico de la democracia." (Recomendación e-democracia 2009, nº 3).

De hecho, se trata de un concepto que afecta a muy variados ámbitos:

"Abarca la E-democracia, en particular, e-Parlamento, e-legislación, e-justicia, e-mediación, e-medio ambiente, e-electorales, e-referéndum, e iniciativa, el voto electrónico, e-consulta, e- peticiones, e-campaña, e-encuestas,

la e-democracia hace uso de la e-participación, e-deliberación y foros electrónicos" (Principio nº 35 Anexo).

En cierto modo, todo el nexo de las materias seguidas en los módulos anteriores de este curso al vincularse con las TICs, valen como un concepto amplio de democracia electrónica.

2. Versión fuerte y versión débil de democracia electrónica

El instrumento que son las TICs bien puede proyectarse en las diversas concepciones de la democracia: tanto en la democracia representativa, la democracia participativa, como en la democracia directa, o más allá de esta terna conceptual, en ámbitos como la llamada democracia social o incluso la empresarial y corporativa. Las TICs son herramientas de comunicación y como tales son medios eficaces para todo proceso participativo de difusión de información y conocimiento, consultas, deliberación, posicionamiento y en su caso, voto.

a) Versión fuerte: e-democracia como democracia directa

Debe advertirse que los estudios sobre democracia electrónica se dan desde mediados del siglo XX. En el tratamiento de la cuestión, hay tanta variedad como autores, en todo caso, puede valorarse de forma genérica el estado de la cuesión. El tratamiento jurídico suele ser escaso y poco profundo, y buena parte de los estudios eran bastante visionarios y utópicos y, por lo general, partían de una crítica –destructiva o constructiva, según los casos- de la democracia representativa, como algo a superar gracias a las TICs. En este sentido, las TICs vienen a ser la *excus*a para cambiar el sistema político. Así las cosas, bajo terminologías diferentes, con la "democracia electrónica" parece latir una apuesta –muy variada- por una democracia directa, en la que cada ciudadano puede expresar instantáneamente, desde su pantalla de ordenador, su punto de vista sobre cuestiones que se sometan a su elección o sobre las que se recabe su opinión, optando a favor o en contra de ellas: una votación continua desde cualquier lugar sobre todos los temas en discusión política. Podríamos decir con Pérez Luño que ésta es una "versión fuerte" de la e-democracia. A mi juicio, vincular las nuevas tecnologías a la democracia directa con votación continua de los asuntos públicos, puede tildarse de "teledemagogia".

Esta visión bastante habitual sobre e-democracia llevaba hasta hace pocos años a que la literatura sobre la materia centre la atención casi monográficamente en el voto telemático o electrónico, descuidando, por el contrario, otros ámbitos esenciales. Ahora bien, estos "expertos" mayormente desconocían la marcha real y usos de la red por los internautas y la ciudadanía,

que les ha sobrepasado por completo por encima. El ciudadano ha pasado a ser el centro de la sociedad de la información en la web 2.0.

b) Versión débil: las TICs como herramienta de mejora de la democracia, no centrada en el voto electrónico.

Como se dijo en el primer módulo, en este curso se apuesta en general por una concepción de la democracia que tienda a ser más deliberativa y más participativa, siempre en el marco de un sistema de democracia representativa e indirecta, que es la que permite el mejor ejercicio y garantía de los derechos fundamentales, vía que ha seguidor la citada Recomendación e-democracia 2009 del Consejo de Europa:

"La democracia electrónica es una oportunidad para permitir y facilitar el suministro de información y deliberación, fomentar la participación ciudadana con el fin de ampliar el debate político, y favorecer un mejor y más legítima decisiones políticas." (Principio nº 9 del Anexo).

No se trata, pues de acabar con la concepción predominante de democracia y suplantarla por otras. De hecho, las democracias representativas deben readaptar su papel, *"Los políticos y los partidos políticos deben aprovechar la e-democracia con el fin de mantener y, si es posible, mejorar su papel esencial como la democracia "intermediarios"... "deben aprovechar las oportunidades que ofrece la e-democracia con el fin de conectar con los ciudadanos y la sociedad que representan, y con compañeros de partido y los órganos del partido." (Criterios 22 y 23 Recomendación e-democracia 2009)*

Las "TICs" no han de ser las protagonistas, sino el *instrumento* de evolución del modelo político. La democracia será lo que las personas queramos, y como afirma Castells, la red será lo que la gente quiera que sea, pues son los usuarios quienes definen su uso. Esta idea también la acoge la Recomendación e-democracia 2009:

"la tecnología más y mejor en sí mismo no conduce a la democracia más y mejor" (Principio nº 49), "La tecnología es de importancia secundaria a las consideraciones democráticas. No debe ser la razón para la introducción de la e-democracia" (Principio 51). Es por ello que "G.1. Al presentar, revisar y mejorar la e-democracia, la atención debería centrarse en la democracia y sus grupos de interés - no en la tecnología." (Criterio nº 1 Anexo).

De igual modo, creo que hay que insistir que la democracia electrónica ni empieza ni acaba, afortunadamente, en el voto electrónico, pese a que hasta la eclosión de la web 2.0 o web social participativa se suelan identificar.

La web 2.0 o web social o participativa, el ciudadano como protagonista activo

La evolución y el uso real y actual de la red obliga a que cualquier referencia a la participación y democracia electrónicas no eluda la realidad del uso ciudadano y participativo de la red en la llamada web 2.0 o web social . Se trata de la superación de la estática web html –que sería el web 1.0-, información dispuesta de forma jerárquica (del creador del contenido hacia el lector pasivo) y no actualizada frecuentemente. Por el contrario, ahora el uso de la web está orientado a la interacción y redes sociales. Los sitios web 2.0 actúan más como puntos de encuentro , bajo una cultura particular, la cultura blog . Me estoy refiriendo a diversos fenómenos comunicativos a través de la red y alternativos a los medios de comunicación tradicionales , como el periodismo alternativo o ciudadano, los blogs , wikis, foros, etc.- o la expresión de movimientos sociales a través de la web 2.0. Frente a la web 1.0, ahora se permite la integración, interacción y selección de contenidos por el usuario (*youtube*, por ejemplo), que deja de ser un receptor, un consumidor de información, sino un "prosumidor" (prosumer) de información, esto es, un híbrido de consumidor y productor de contenidos , en deliberación continua. También, redes sociales como *Facebook* o *Tuenti* son ejemplos de la web 2.0 en su fenómeno de crecimiento geométrico de las redes sociales. El éxito de la web social estriba, en buena parte, en la gran facilidad de las nuevas herramientas. En todo caso, no hay que olvidar que a diferencia de la web 1.0 el usuario no es pasivo sino activo y requiere de unas destrezas importantes, lo cual agrava la importancia de la alfabetización digital y la posible discriminación de los desconectados.

Como hito de este proceso, la declaración de personaje del año de Time en 2006

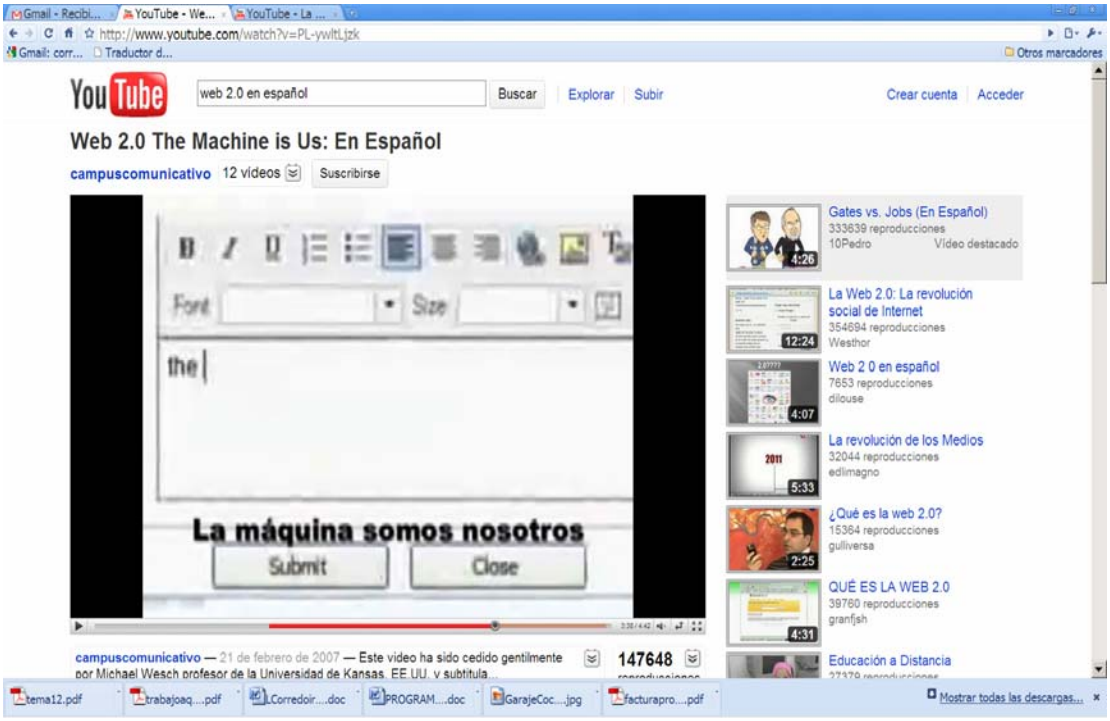
Las TICs facilitan el empoderamiento del ciudadano, la construcción desde abajo arriba, el control de la información así como "la e-democracia debe permitir más participación del ciudadano en establecer la agenda, el análisis y la formulación, ejecución y seguimiento de la política." (Directriz nº 7 Recomendación e-democracia 2009).

""la e-democracia puede ser introducida por cualquier interesado. Puede ser iniciada de arriba hacia abajo, es decir, por las autoridades públicas, en todos los niveles de gobierno, o de abajo hacia arriba, es decir, por los ciudadanos. También puede ser de diseño horizontal. Cada enfoque tiene sus méritos." (Principio nº 59).

La noción de web 2.0 es ciertamente interesante para la comprensión de la e-democracia.

Cabe seguir algunos recursos visuales:

(subtitulado) http://www.youtube.com/watch?v=PL-ywltLjzk



En español http://www.youtube.com/watch?v=OwWbvdllHVE&feature=related

3. Conceptos afines: especial atención al "gobierno electrónico" y la actual tendencia hacia la "administración 2.0

Hay diversos conceptos de especial interés y afinidad para la materia abordada.

El concepto de "TICs" desde los años 70 se utiliza para indicar la convergencia que culmina en los años 90 de la electrónica, la informática, las telecomunicaciones. Se hace referencia a aquellas tecnologías que permiten la adquisición, almacenamiento, procesamiento y comunicación de datos en informaciones -textos, voz, imágenes,...etc.- contenidos en señales de naturaleza acústica, electromagnética u ópticas. Aunque no exclusivamente, hoy día internet es emblema de las TICs y concentra toda la atención.

"Sociedad de la Información" "es una fase de desarrollo social caracterizada por la capacidad de sus miembros (ciudadanos, empresas y administración pública) para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera". (Fundación Telefónica, accesible en http://www.telefonica.es/sociedaddelainformacion/espana2000/pdfs/parte1.pdf).

"Sociedad del conocimiento": se alcanza cuando los datos y la información se integren en un marco que permite hacer un uso eficiente y eficaz del gran caudal de los mismos y generar conocimiento "ex novo", lo cual requiere el proceso, análisis, clasificación, reflexión y asimilación de la información, convirtiéndola en acción mediante la toma de decisiones.

Asimismo, procede hacer referencia a algunas definiciones de gobierno o administración electrónica (*egovernment*, indistintamente en inglés). Y es que el mismo concepto viene vinculado a la participación y democracia a través de las TICs.

De entre las diversas definiciones, cabe destacar la que sigue "es el uso de las tecnologías de información y comunicaciones que realizan los órganos de la administración para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos".

Proyecto de Reforma y Modernización del Estado. Gobierno electrónico en Chile hoy. Ministerio Secretaría General de la Presidencia pp 2.

http://hasp.axesnet.com/contenido/documentos/Libro%20Estado%20del%20Arte%20del%20E-Gob%20en%20Chile.pdf

La conexión clara se produce al considerarse el e-gobierno como una evolución, que resumidamente cabe exponer:

1- Acceso y accesibilidad a la información sobre y de la administración.

2- Interacción básica, caracterizada en muy buena medida por la posibilidad

de comunicación del administrado con la administración.

3- Interacción avanzada en ambos sentidos administrado-administración, hasta la prestación total de servicios y plena tramitación.

4- Formas de participación y democracia digital.

Según lo dicho, incluso se podría afirmar el continuo lógico de estas nociones:

e-administración → e-gobierno → e-participación → e-democracia

A partir de las nociones web 2.0 y e-gobierno, en la actualidad esta muy en boga la idea de "administración 2.0" o "e-gov 2.0", lanzada por expertos como David Osimo (http://egov20.wordpress.com/). Desde estos movimientos se ha influido en la Declaración Ministerial sobre administración electrónica aprobado por unanimidad en Malmö, Suecia, el 18 de noviembre 2009.
http://ec.europa.eu/information_society/activities/egovernment/conferences/malmo_2009/press/ministerial-declaration-on-egovernment.pdf

Entre otras ideas se insiste en la necesidad de centrar la e-administración en el ciudadano mediante servicios flexibles y personalizados, productos de información basados en la demanda (user-centry); la usabilidad de las aplicaciones de e-administracion, la necesidad de involucrar a la sociedad y que ésta evalúe los servicios públicos electrónicos. De igual modo se invita a que los particulares estimulen y colaboren en la prestación de tales servicios. También es esencial a la idea de adminstración 2.0 la transparencia, "Vamos a explorar cómo podemos hacer que nuestros procesos administrativos sean más transparentes" (nº 12) y la apertura y participación "pública a través de métodos más eficaces en todos los niveles del gobierno" (nº 13).

2. Aprehensión jurídica general del fenómeno

1. Ventajas generales de las TICs para la democracia y gobierno

Se pueden alegar una infinidad de ventajas para la implantación de la democracia, la participación y el gobierno electrónicos:

Eficacia: más eficacia en la prestación de servicios públicos, vinculados también a la democracia y participación. Mejor funcionamiento de sistemas electorales, facilidades para mejor ejercicio y funcionamiento de la administración electoral. Facilitación de implantación de mecanismos de acceso a la información y participación en diversos niveles, etc.

Eficiencia: lograr la eficacia a menor coste. Así sucede por ejemplo en procedimientos electorales y administración electoral y, sobre todo, en la facilitación de acceso a la información pública a través de la red, también como canal de participación variada pública o privada.

Transparencia: en principio por una información pública al público más accesible, con diversos niveles de profundidad.

Comodidad, para el ciudadano al que se le añade un canal de información y participación fácilmente disponible desde un punto de acceso informático, generalmente doméstico.

Pluralismo: la pluralidad inherente a la red facilita en principio el mayor pluralismo y que los medios de comunicación clásicos (públicos o privados) , en ocasiones oligárquicos, dejen de constituir un filtro material al libre flujo de información y opinión.

Participación y cultura participativa: las anteriores ventajas, en principio facilitan un aumento de participación por la comodidad de hacerlo para el ciudadano y por la ampliación de posibilidades de llevarlo a cabo.

Inclusión: permite añadir participantes en sectores específicos con tradicionales dificultades (enfermos, discapacitados, emigrantes, desplazados, etc.). Facilita el interés, la información y las posibilidades en algunos sectores sociales así como en territorios con dificultades de acceso y movilidad.

Permite la estructuración de la participación política de los ciudadanos y los grupos en los que se integra: la red permite que colectivos, grupos e individuos se articulen de manera antes desconocida a través de la red, compartan información, deliberen, actúen y participen (asociaciones formales o no, redes ciudadanas, nuevos movimientos sociales temporales o permanentes, etc.).

Facilita la memoria política: la ingente información de la red, su estructuración y permanencia (por ejemplo a través de Google, permite recuperar la memoria política de acontecimientos pasados de trascendencia (afirmaciones de responsables políticos, etc.).

2. La obligación de implantar formas de e-democracia y e-gobierno como principio jurídico-constitucional, concretable por un legislador con voluntad política

Tanto desde la perspectiva de la administración electrónica, como desde una perspectiva más cercana a la democracia y participación electrónicas, ventajas como las anteriormente enunciadas llevan a afirmar que hay un principio jurídico-constitucional objetivo que impulsa a los poderes públicos a adoptar políticas en la dirección de la implantación del gobierno, democracia y participación electrónicas. Así, por ejemplo, todos los documentos resultantes de la Cumbre Mundial sobre la Sociedad de la Información (CMSI, Ginebra, 2003, y Túnez, 2005). En español: http://www.itu.int/wsis/index-es.html

Según las constituciones de cada país, este principio objetivo puede encontrarse, por ejemplo, en los mandatos de eficacia y democracia del gobierno y la administración, de buena administración, de servicio a los ciudadanos, de acceso a la información pública y de transparencia, etc. Asimismo, según lo que

concretamente quiera sostenerse este principio objetivo puede considerarse en el marco de la dimensión objetiva de algunos derechos fundamentales, como el derecho al sufragio activo y pasivo, el derecho de participación general, el derecho de petición, el libre acceso a la información (en su caso pública), la libertad de expresión, el derecho de educación, el derecho a la buena administración, derecho de acceso a los registros o archivos, el derecho de audiencia previa a las decisiones y cualquier otra forma jurídica que adquieren derechos subjetivos vinculados al ámbito de la democracia y participación.

En ocasiones, no es descartable que las constituciones y otras normas jurídicas incluyan referencias expresas a las nuevas tecnologías y el deseo de implantación en la administración, poderes públicos y mecanismos participativos. Muchas veces las normas afirman las ventajas de las TICs o formulan derechos que no tienen la estructura de tales, por lo que se hacen difícilmente exigibles o generan sólo obligaciones genéricas para los poderes públicos. No es impensable, sin embargo, que la jurisprudencia futura reconozca exigencias concretas de implantación de democracia y gobierno electrónicos como parte del contenido subjetivo sí directamente exigible de algunos derechos fundamentales.

Ahora bien, el legislador en ocasiones adopta compromisos concretos y exigibles. Como ejemplo en España, el artículo 6 de la Ley 11/2007 sobre e-administración que reconoce un auténtico derecho:

"Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos."

Al fin y al cabo, todo depende de la voluntad política, "*la e- democracia prospera mejor donde hay la voluntad política y liderazgo para hacer que funcione con eficacia mediante la introducción de los cambios estructurales necesarios para tener en cuenta las opiniones expresadas. La incorporación de las TIC en los procesos democráticos por lo general requiere cambios estructurales y la reforma procesal." (Recomendación e-democracia 2009, Principio nº 63).*

Por múltiples motivos, es cierto que el Derecho recibe mal y tarde la incuestionable implantación y evolución de las nuevas tecnologías: dinamismo, variabilidad técnica, desconocimiento, costes, necesidad de reposo que exige el Derecho, etc.

No obstante, es posible imponer compromisos y obligaciones concretas a través del Derecho. El ejemplo más llamativo y relevante para la materia de transparencia y democracia electrónicas es el que se produjo tras la quiebra de la

empresa norteamericana Enron (http://es.wikipedia.org/wiki/Enron) a principios de la década. Y es que desde entonces se ha producido una ola legislativa por la que se exige una muy elevada transparencia –también a través de internet- y la implantación de mecanismos de participación telemática, a grandes empresas cotizadas en bolsa en favor de la transparencia económica. La crisis financiera de 2008 y el escándalo del caso Madoff (http://es.wikipedia.org/wiki/Bernard_Madoff), a buen seguro supondrá un nuevo impulso a la transparencia financiera. Estas son buen ejemplo de que sí posible exigir jurídicamente obligaciones concretas de transparencia e información pública, que "sólo" habría que trasladar a los distintos poderes públicos. Y es que lo irónico es que por lo general los poderes públicos no se obligan jurídicamente a ellos mismos a facilitar información pública por medios electrónicos ni facilitar la participación y apertura.

3. Acceso a las TICs, brecha digital y su tratamiento jurídico

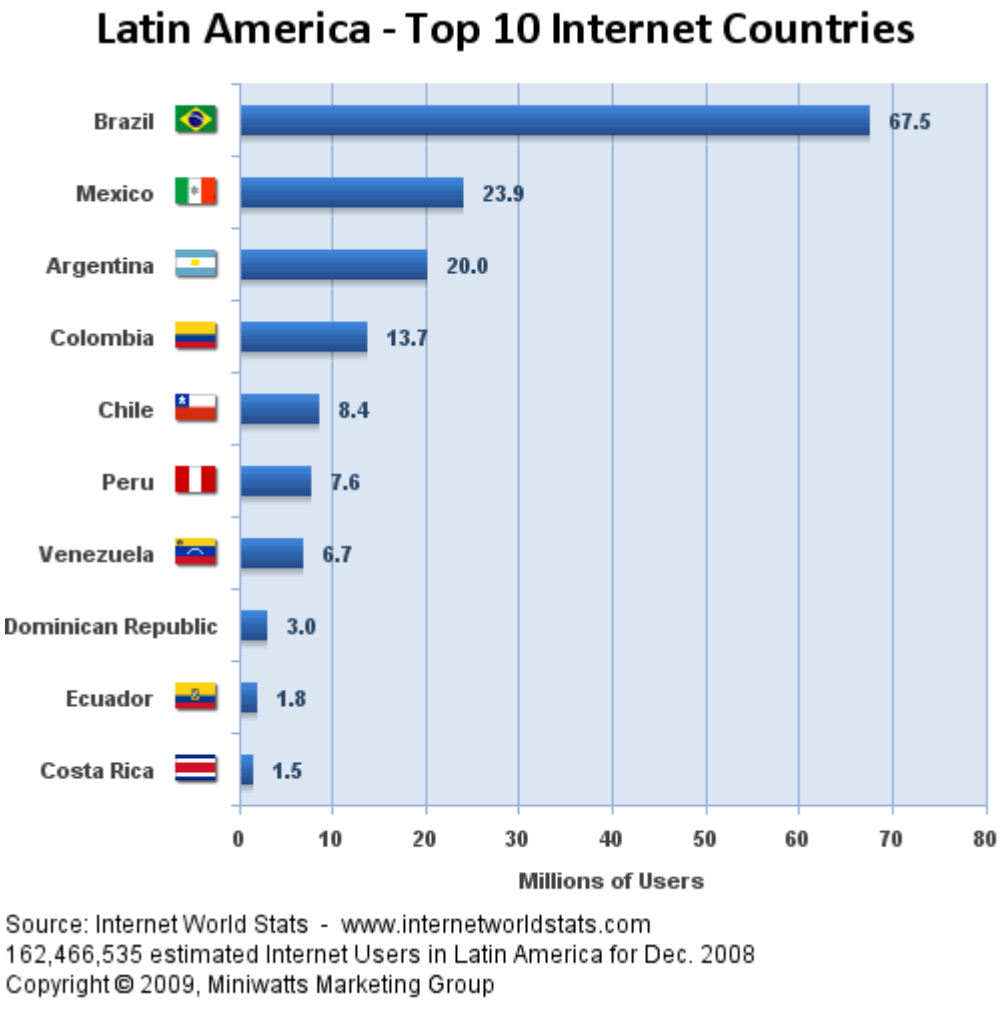
1. Acceso a internet en Latinoamérica y España

Los datos más recientes (diciembre de 2009, http://www.internetworldstats.com/stats.htm) señalan que un 32,1 % (14,4% en marzo de 2006) de la población de América Latina (sin Caribe) están ya conectados a internet. El total de los internautas mundiales es aproximadamente de mil ochocientos millones. La media de acceso en Europa, según esos datos es de 53 %, la Unión Europea de 27 el 59% y de Norte América 76, 2% (68.6% en 2006).

WORLD INTERNET USAGE AND POPULATION STATISTICS					
World Regions	**Population (2009 Est.)**	**Internet Users Dec. 31, 2000**	**Internet Users Latest Data**	**Penetration (% Population)**	**Growth 2000-2009**
Africa	991,002,342	4,514,400	**86,217,900**	8.7 %	1,809.8 %
Asia	3,808,070,503	114,304,000	**764,435,900**	20.1 %	568.8 %
Europe	803,850,858	105,096,093	**425,773,571**	53.0 %	305.1 %
Middle East	202,687,005	3,284,800	**58,309,546**	28.8 %	1,675.1 %

North America	340,831,831	108,096,800	**259,561,000**	76.2 %	140.1 %
Latin America/Caribbean	586,662,468	18,068,919	**186,922,050**	31.9 %	934.5 %

Por países, en América Latina (http://www.internetworldstats.com/stats10.htm#spanish), en febrero 2009 destaca la penetración de internet en Chile 44,9 % (35.7% en 2006) o Argentina 39,3% (26.4% en 2006). Por orden de penetración de internet: Chile 44.9 %; Argentina 39.3 %; Costa Rica 35.7 % (22.7% en 2006); Uruguay 31.6 %(20.8% en 2006); Colombia 30.5 %(9.7% en 2006); Peru 26.2 % (16% en 2006); Brazil 26.1 %(14.1% en 2006); Puerto Rico 25.3 %; Venezuela 22.5 %(12% en 2006); Dominican Republic 22.1 %; Mexico 21.6 % (16.2% en 2006); Guatemala 10.2 %; El Salvador 9.9 %; Ecuador 8.0 %(5.2% en 2006); Panama 8.0 %; Bolivia 6.3 %(3.8% en 2006); Honduras 4.5 % (3.3% en 2006); Paraguay 3.8 % (2.7% en 2006; Nicaragua 2.7 %(Nicaragua 2.2% en 2006) y finalmente en la cola, Cuba con un 2.1 %.



En España, los conectados a internet son el 63,3% (38.7% en 2006), ocupando un lugar medio en la Unión Europea ampliada a 27 (59 %) frente a países como Holanda (90%) o Noruega (87,7%). Ahora bien, España se sitúa bastante por encima de la media latinoamericana. En diciembre de 2009 el grado de penetracion es del 71, 8 % en España.

Sin perjuicio de que los datos de Latinoamérica puedan llevar a relativizar la cuestión que aquí se afronta, debe tenerse en cuenta un significativo crecimiento. Así, para Latinoamérica es especialmente llamativo el índice de crecimiento de 2000-2005, el segundo en el mundo al multiplicarse el uso de la red en 3.42 veces. En el periodo 2000-2008, el crecimiento de la zona ha sido de 8,2 veces.

Ahora bien, debe tenerse en cuenta que se trata de datos de acceso a internet, sin que pueda considerarse que los usuarios conectados sean capaces de hacer un uso funcional y eficaz de la red, como el que requieren en los más de los casos las diversas formas de participación y democracia electrónica.

También, a falta de datos concretos para Latinoamérica, debe tenerse en cuenta que los estudios generales muestran cómo los accesos –y más los usos eficaces de internet- se dan entre los sectores medios y altos de la población, más entre hombres que entre mujeres, más entre jóvenes que mayores, más en zonas urbanas que en zonas rurales. Como se ha adelantado, el uso algo avanzado es capital para la web social participativa o web 2. 0.

Hoy por hoy la red reproduce, incluso intensifica las pautas de marginalidad social no virtuales. Y no cabe duda de que se trata de un factor nada despreciable cuando se trata de la democracia y participación electrónicas.

2. Brecha digital y elitocracia electrónica

Por lo expuesto, un peligro de obligatoria advertencia y atención jurídica es el de una dualización (conectados/desconectados), la llamada "informarginalidad", "muro", "telón" o, más habitual, "brecha digital" tanto social o territorial y su obvia conexión con la implantación de la democracia y participación electrónicas.

> Los sectores más marginados y necesitados de representación de intereses y de conformación de interés general sobre la base de sus necesidades son los que menos acceden a la red o lo hacen con menor eficacia. De ahí, que al igual que en la implantación de servicios públicos a través de internet ha de tenerse especial cautela con la no discriminación. Ello conduciría, como diversos autores han alertado a una democracia de elites.
>
> Desde el punto de vista jurídico, el tratamiento puede venir dado desde el principio de igualdad y los derechos fundamentales (y su dimensión institucional y prestacional).

a) No discriminación en la implantación del gobierno y democracia electrónicas

Desde la igualdad, debe garantizarse que la implantación de servicios electrónicos no genere discriminaciones. Ahora bien, el avance de las nuevas tecnologías siempre va a dotar de más posibilidades a quien accede a las mismas que a quien no quiere o no puede hacerlo. El ciudadano conectado, lógicamente, siempre contará con más y mejor información. Considerar esto discriminatorio por sí frenaría, de forma absurda, el avance de la sociedad de la información y conocimiento. En general, dotar de ventajas al internauta no debe considerarse discriminatorio, siempre que ello no implique una clara desventaja, incluso castigo a quien no está conectado. El tratamiento jurídico no es en modo alguno sencillo y es preciso ir al caso concreto.

En este punto, las acciones presuntamente discriminatorias se dan cuando no se duplican las ventajas de la red en el mundo no virtual y, sobre todo, la discriminaciones pueden provenir de la imposición de interactuar sólo electrónicamente. Como ejemplo, el artículo 27. 6º de la ya referida Ley 11/2007 española sobre e-administración:

"6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos."

Estas medidas deben ir acompañadas de garantías de acceso a todos a las TICs (art. 8):

"1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada."

Según lo visto, basta un reglamento para imponer la obligación de relacionarse electrónicamente con la Administración. Por ejemplo, millones de pequeñas empresas o empresarios autónomos, o comunidades de propietarios quedan obligados a ser notificados electrónicamente de, por ejemplo, las multas de tráfico o comunicaciones con Hacienda, respectivamente.

No obstante, no puede ser automático considerar discriminatoria esta imposición de relacionarse electrónicamente. Esta evaluación jurídica debe hacerse sobre todo desde los parámetros del derecho a la igualdad, reforzada jurídicamente su garantía en conexión con el derecho o libertad de que se trate (derecho de sufragio, general de participación, derecho de acceso a la información pública, derecho de petición, etc.). Pueden tenerse en cuenta especialmente dos elementos, uno formal y otro material:

-garantías formales: facilita la admisibilidad de la imposición de la interactuación electrónica que ésta venga fijada en ley formal, sin perjuicio de que luego remita al desarrollo reglamentario. Mayor legitimidad contará en cuanto la regulación legal concrete en mayor medida las condiciones para que sea obligatoria la interactuación electrónica y fije los espacios que debe concretar una norma inferior. Así, la norma legal puede fijar pautas a la norma inferior de quién, cuándo, cómo y porqué puede exigirse la interactuación electrónica.

-garantías materiales: las normas que fijen la interactuación obligatoria, deberían determinar con una certeza mínima el colectivo de personas u organizaciones a los que se obliga a la interactuación electrónica. El acierto y certeza en su fijación pueden ser un criterio determinante para la admisión de la medida desde las pautas de razonabilidad. Asimismo, deben contener previsiones para evitar posibles situaciones y dificultades concretas, como la garantía de acceso a puntos de internet, garantías técnicas frente a caídas del servicio, asistencia técnica, etc.

b) Las políticas de acceso a internet y alfabetización digital. ¿Un derecho fundamental al acceso a la sociedad del la información?

En todos los sistemas constitucionales no faltan anclajes jurídico-constitucionales para apoyar jurídicamente todas las políticas conducentes a facilitar la sociedad de la información y del conocimiento, la alfabetización digital y el acceso a internet por la ciudadanía: afirmación de la igualdad material, derecho a la educación y dimensión objetiva y prestacional de los derechos fundamentales, en especial, derechos de información y comunicación, etc.

Cada vez tiene más acogida la afirmación de un derecho a la comunicación (*ius comunicationis, los"Communication Rights*) de naturaleza constitucional o casi-constitucional. El artículo 19 de la Declaración Universal de Derechos Humanos que en su artículo 19 se afirma que: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." Este artículo, con sus sesenta años a la espalda puede –y debe- interpretarse en

clave de la sociedad de la información. Así lo hace Naciones Unidas en la *Declaración de Ginebra*, 2003 y la *Declaración de Principios* Túnez en Noviembre de 2005 (http://www.itu.int/wsis/index-es.html). Sin valor jurídico son referentes donde se afirma el "derecho de acceso como acceso universal".

En España el *ius comunicationis* ha tenido clara acogida en algunos Estatutos de autonomía (máxima norma institucional de las regiones). Así, destaca el Estatuto de la Comunidad Valenciana en su artículo 19. 2º: "*Queda garantizado el derecho de acceso de los valencianos a las nuevas tecnologías y a que La Generalitat desarrolle políticas activas que impulsen la formación, las infraestructuras y su utilización.*" Se trata de muestras o expresiones del alcance de este nuevo derecho, pero más como principios que como derechos subjetivos exigibles. De hecho, éstas y otras proclamaciones tienen singular valor jurídico en sentido negativo, pues valen especialmente como apoyo jurídico para la adopción de medidas de implantación de políticas de universalización del acceso a internet, de extensión territorial o social de servicios, etc. Sin embargo, es bastante discutible que se generen derechos subjetivos para los particulares de que el Estado les garantice acceder a la red, recibir formación digital, etc. Cuestión diferente, como se verá, es la del derecho fundamental en juego ante medidas que suponen la restricción del acceso a la red, en las que sin duda está en juego la libertad de expresión e información como derecho subjetivo.

4. Administración electoral y TICs, las TICs en las campañas electorales

1. Administración electoral y la creciente emergencia de las TICs en campaña

El empleo de las TICs es una realidad en cualquier sector, y también en la organización y procedimiento electorales. En el ámbito de las actuaciones de administraciones electorales son diversas los reflejos de las TICs. Así, es posible la comprobación electrónica de la corrección del censo por los ciudadanos electrónicamente.

https://censoelectoral.ine.es/censo/ce_internet1_noelectoral.menu

En diversos países de América Latina el uso de censos electorales electrónicos añade algunas funcionalidades. Resultan a mi juicio peligrosas las funcionalidades que añaden automáticamente en el censo electoral los registros de si el ciudadano ha votado a cada comicio, incluso en tiempo real el día de las elecciones. Ello tiene ventajas en la depuracion y actualización del censo o padrón. Sin embargo, el conocimiento automatizado del comportamiento electoral del electorado permite un peligroso y abusivo control por gobiernos, partidos y cantidatos. Ello facilita, por ejemplo, tratamientos específicos por

candidatos o partidos de los votantes según su carácter mas o menos abstencionista.

De otro lado, se ha señalado con acierto que las administraciones electorales van a tener que añadir en su composición a técnicos en TICs que garanticen, vigilen, resuelvan -y expliquen a los miembros no técnicos- las nuevas cuestiones relativas al voto electrónico, *software* empleado, etc.

No procede ahora recordar todas las posibilidades que la red permite para la difusión de información, la deliberación, la movilización de recursos económicos, personales y emocionales entre la población, en especial, la población internauta. Se dice, con diversa fundamentación sociológica y politológica, que los *blogs* (a modo de páginas web personales) en EEUU marcaron la agenda política durante el último semestre de las elecciones Bush vs. Kerry en 2004 y, finalmente, decidieron la victoria, gracias al predominio republicano en la red, superando la incidencia de los medios de comunicación clásicos. En las elecciones presidenciales EEUU de 2008, la fuerte presencia de Obama en las reces sociales, con centenares de miles de "amigos" en *Facebook* por ejemplo, fue un elemento más para su victoria[1].

Al respecto, http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

Aunque pueda sorprender, los elementos básicos del uso de la red en campaña electoral ya los empleó un personaje como Jesse Ventura (ex lucha libre y sustentador de numerosas teorías de la conspiración) para lograr el puesto de Gobernador de Minessota en 1998 sin ser de partido mayoritario alguno. Recientemente, movimientos sociales en la red han desembocado, por ejemplo, en el "Tea Party" (http://en.wikipedia.org/wiki/Tea_Party_movement), con logros como arrebatar para el Partido Republicano un senador en Boston, lo que no se lograba en 50 años.

2. Novedades en internet por cuanto a típicas prohibiciones previas a los comicios electorales

Como es de sentido común, "las limitaciones establecidas por la legislación electoral son también aplicables al uso de este tipo de medios electrónicos" (Exposición de Motivos Instrucción 4/2007, de 12 de abril, de la Junta Electoral Central).

http://www.juntaelectoralcentral.es/portal/page/portal/JuntaElectoralCentral/JuntaElectoralCentral/DocJEC/Instrucciones/12042007

[1] A texto completo, puede seguirse http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

a) Internet y jornada de reflexión electoral:

Es típico en muchos países la existencia de un periodo de prohibición de la solicitud del voto. Esta prohibición en general debe trasladarse a internet, así como las posibles sanciones por su incumplimiento.

Ahora bien, debería en todo caso tenerse en cuenta la necesidad de adecuar y flexibilizar criterios para juzgar su posible incumplimiento en internet. Por lo general, debe seguir prohibiéndose cualquier fórmula activa de promoción del voto en internet, no requerida por el usuario (por ejemplo mensajes emergentes, correos electrónicos). También, debe considerarse prohibida la publicidad en medios clásicos de comunicación en internet que se actualizan frecuentemente (por ejemplo, un periódico en internet). Por el contrario, la prohibición debe relativizarse y flexibilizarse para modos de comunicación en internet que siguen accesibles el día de la prohibición, en los que retirar los contenidos prohibidos exigiría importantes esfuerzos para su eliminación (foros, webs de partidos pequeños sin medios, páginas personales de partidarios de un sentido del voto, etc.).

En este punto, debe tenerse en cuenta la actividad positiva del internauta que voluntariamente accede a estos sitios.

b) Prohibición de encuestas y sondeos

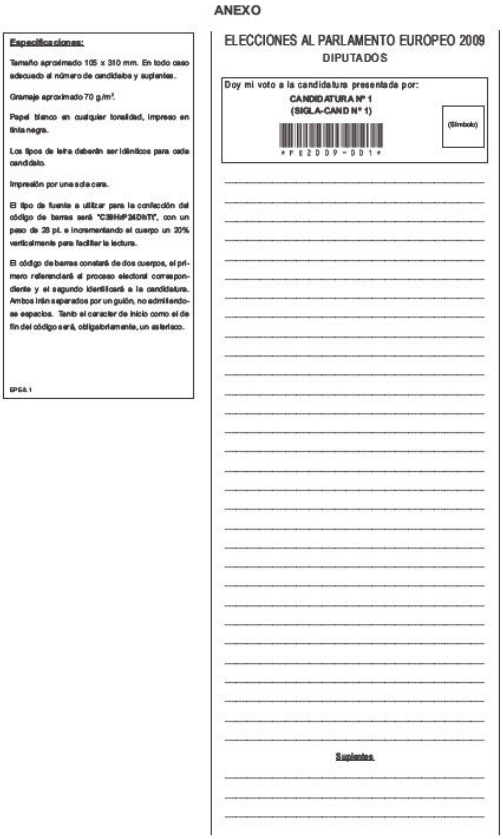
Se suscitan problemas fácticos también por cuanto a la prohibición de realización y publicación de encuestas y sondeos electorales durante un periodo previo a la elección, algo común en diversos países. Dicha obligación es fácilmente eludida cuando la información prohibida se ubica en medios de comunicación no sometidos a la legislación –o a la acción- del país de que se trate. El ciudadano internauta del territorio donde rige la prohibición puede fácilmente acceder a tales contenidos prohibidos, lo cual es difícilmente evitable, e incluso resultaría desproporcionada la mera amenaza al usuario de que su acción es ilícita. Por ejemplo, en las elecciones generales de 2008 en España, la semana de prohibición de difusión de sondeos, algunos periodicos online incluyeron un enlace en su portada en la red hacia sondeos publicados por medios situados en Andorra (muy pequeño país fronterizo con España), por ejemplo. La prohibición española, obviamente, no alcanzaba a aquel país.

5. Voto electrónico: tipos y garantías

1. Voto electrónico y su tipología: una importante distinción

La informatización del proceso electoral no es en modo alguno nueva. No en vano la concentración de resultados se realiza normalmente de forma electrónica, si bien, el rastro en papel se conserva para verificar datos y efectuar los oportunos recuentos. Aquí se analiza especialmente la introducción de dispositivos electrónicos en el momento en el que ciudadano emite su voto. Y hay que añadir que el uso de máquinas para la votación tampoco es nuevo, se remonta a fines del siglo XIX en EEUU. Máquinas de votación por palanca o con perforadores no son nuevas. Lo nuevo, y en ello se centra el análisis del e-voto estriba en la desmaterialización física del voto que hace difícil o imposible comprobar los resultados sobre la base del voto emitido puesto que los votos quedan guardados en soporte electrónico y el elector no puede comprobar por sí mismo la corrección de la votación.

En este punto, por ejemplo, cabe señalar las papeletas electrónicas recientemente introducidas en España, las mismas facilitan el escrutinio, pero el soporte sobre el que se basa el escrutinio sigue siendo el papel, no la información electrónica. Se trata del escrutinio electrónico *e-counting*, pero no del voto electrónico. A diferencia de este supuesto son los casos en los que aun siguiendo un posible rastro en papel (a efectos de detectar discrepancias o dejar resguardos para el votante, el resultado de la votación proviene de la información electrónica.


ANEXO

Especificaciones:

Tamaño aproximado 105 x 310 mm. En todo caso adecuado al número de candidatos y suplentes.

Gramaje aproximado 70 g/m².

Papel blanco en cualquier tonalidad, impreso en tinta negra.

Los tipos de letra deberán ser idénticos para cada candidato.

Impresión por una sola cara.

El tipo de fuente a utilizar para la confección del código de barras será "C39HrP24DhTt", con un paso de 28 pt. e incrementando el cuerpo un 20% verticalmente para facilitar la lectura.

El código de barras constará de dos cuerpos, el primero referenciará al proceso electoral correspondiente y el segundo identificará a la candidatura. Ambos irán separados por un guión, no admitiendose espacios. Tanto el carácter de inicio como el de fin del código será, obligatoriamente, un asterisco.

EP/G.1

ELECCIONES AL PARLAMENTO EUROPEO 2009

DIPUTADOS

Doy mi voto a la candidatura presentada por:

CANDIDATURA Nº 1

(SIGLA-CAND Nº 1)

(Símbolo)

PE2009-DD1

Suplentes

Imagen: ejemplo de modelo de papeleta, con código electrónico

Una vez centrada la noción de voto electrónico, es especialmente necesaria una precisión conceptual sobre el voto electrónico y su tipología. Tales distinciones tienen una también muy diversa en el sistema político y en su tratamiento jurídico-constitucional.

a) Voto electrónico local en entornos sí controlados

Se trata del uso de medios electrónicos de votación en entornos controlados oficialmente, como los colegios tradicionales de votación o, en general, en cualquier otro lugar que cuente con suficiente supervisión a cargo de la administración organizadora. Así, se hace referencia al voto a través de papeletas ópticas (sus datos son grabados por un lector óptico, por ejemplo, códigos de barras). De igual modo, el voto en urnas que son ordenadores: se vota con botones, lápiz óptico o la misma mano. El voto queda registrado en el ordenador, implica la supresión de las papeletas tradicionales como medio de votación, aunque es posible que estas máquinas emitan un comprobante en papel.

Así las cosas, vemos que es muy posible hacer referencia al "voto electrónico" a supuestos en los que poco o nada cambia el sistema electoral al exigirse unas fuertes medidas de control sobre el proceso y, sobre todo, no se trata de voto telemático que permita al votante no acudir al lugar controlado.

Estas modalidades están muy generalizadas precisamente en diversos países de Latinoamérica, como Brasil. En dicho país se ha ido extendiendo en los últimos veinte años, al punto de alcanzar el 100% de las votaciones y regularse como excepcional y subsidiario el voto no electrónico (art. 59 Ley nº 9504, de 30 de septiembre de 1997). En Venezuela comenzó a emplearse en 1998 (a partir del impulso de la Ley Orgánica del sufragio y participación política, de 13 de diciembre de 1997) y se generalizó su uso en el refrendo revocatorio de 2004. Por lo general se extiende la modalidad llamada "RED" (Registro Electrónico Directo, *Direct Recording Electronic*): el voto se registra directamente en la memoria de la urna electrónica (esta modalidad se prevé en Perú, República Dominicana, Panamá y Colombia).

Entre las modalidades, cabe señalar el voto por computadora, con al menos un dispositivo para elegir la candidatura y otro para emitir el voto. Se necesita la conexión entre la mesa electoral y el votante tanto para asistirle como para evitar fraudes de este último. Como recuerda Barrat:

"las máquinas holandesas *Nedap* incorporan, por ejemplo, dispositivos sonoros y, en México, el *Instituto Electoral del Distrito Federal* (IEDF) ha desarrollado un máquina de votación que solo puede activarse apretando un botón que se encuentra a disposición de la Mesa electoral y está conectado con un cable con la propia máquina. *Indra*, por último, utiliza tarjetas anónimas que se proporcionann al elector una vez que se ha identificado, en Coahuila (México) se proporcionan con objetivos similares recibos con código de barras y *Scytl* facilita a los electores código alfanuméricos que deben introducir en la pantalla de votación."

Por cuanto al método de elección de candidaturas, hay sistemas como Venezuela en el que el lector ve una papeleta –en papel- como la tradicional, sobre un un dispositivo electrónico sensible al tacto y capaz de transmitir estos impulsos a la urna propiamente dicha. La máquina recibe la opción y el elector confirma que ésa era la opción deseada.

b) Voto electrónico telemático, "pyjama voting" a distancia en entornos no controlados

El voto electrónico en entornos controlados, no a distancia guarda escasas diferencias con el voto no electrónico y poco o nada altera sistema político, sólo facilita el proceso electoral. Está claro que la potencialidad de las TICs respecto del e-voto lo es por cuanto el voto a distancia, telemático, desde cualquier lugar.

El voto telemático electrónico es habitual en ámbitos no reglados, como votaciones a concursos de televisión a través de mensajes por teléfono móvil. Incluso algunas actuaciones administrativas pueden realizarse también

expresando el consentimiento por vía de mensajes SMS desde celulares. Se trata de actuaciones de mayor o menor relevancia social o administrativa, pero que en modo alguno exigen las garantías políticas y jurídicas de un sufragio electoral.

De igual modo, el voto telemático electrónico en entornos no reglados ya es una realidad en el mundo empresarial, donde las garantías no se requieren con la intensidad que en el ámbito electoral general de la política pública. Incluso en algunos casos, normativas de transparencia para el mundo empresarial y societario exigen su implantación. Por el contrario, esto no sucede cuando se trata del derecho de voto político.

El voto telemático electrónico es habitual en ámbitos no reglados, como votaciones a concursos de televisión a través de mensajes por teléfono móvil. Incluso algunas actuaciones administrativas pueden realizarse también expresando el consentimiento por vía de mensajes SMS desde celulares. Se trata de actuaciones de mayor o menor relevancia social o administrativa, pero que en modo alguno exigen las garantías políticas y jurídicas de un sufragio electoral. De igual modo, el voto telemático electrónico en entornos no reglados ya es una realidad en el mundo de las sociedades anónimas , donde las garantías no se requieren con la intensidad que en el ámbito electoral general de la política pública. Algunos países ya lo regulan como algo a implantar en el futuro (como Colombia, Ley 892 de 2004, para ciudadanos en el extranjero) o se detectan proposiciones de ley, como recientemente Francia para ciudadanos en el extranjero (Ley modifica la Ley orgánica nº 76-97 de 1976, 31 de enero sobre el voto de los franceses residentes en el extranjero para las elecciones del Presidente de la República). Lo más llamativo en todo caso es la puesta en práctica real de este sistema en Ginebra en 2004 , un lugar donde un 90% de los ciudadanos ya ejercía el voto por correo –sin garantías de certificado- y que se habilita el voto telemático con iguales garantías que el voto por correo. Asimismo, y de mayor relevancia, resulta el caso de Estonia, después de las elecciones locales de 2005, en marzo de 2007 y para elecciones parlamentarias un 3% de los ciudadanos votaron a través de un portal habilitado al efecto. Requerían su documento de identidad, la firma electrónica y un contraseña en un ordenador dotado de un lector electrónico de tales elementos . La clave: el avanzado estado letón en la implantación de la administración electrónica y la plena confianza en el sistema, pese a que las garantías reales hoy por hoy son muy discutibles.

Ahora bien, hoy por hoy, todo parece indicar que las tecnologías no permiten el mismo aunando las garantías exigibles en un proceso electoral democrático. Así, el proceso más ambicioso de voto a distancia, telemático –no sólo electrónico- fue un rotundo fiasco (*Secure Electronic Registration and Voting Experiment* (SERVE), promovido por el Gobierno de Estados Unidos para quienes estuvieran fuera del país, como militares. Por ello, hoy día se sigue prefiriendo el voto postal por las garantías que presenta. En todo caso, las

experiencias son continuas en diversos países y no se sabe lo que el futuro ha de deparar.

2. Las garantías constitucionales del voto electrónico: los "principios" del Consejo de Europa

Son diversas las normas que regulan las posibilidades y garantías del voto electrónico, casi siempre, con exclusiva referencia al voto local en entornos controlados, no a distancia o telemático. Sobre la proyección de las garantías constitucionales tradicionales, ínsitas en el mismo contenido del derecho al sufragio activo o pasivo, parece conveniente remitirse a la Recomendación del (2004)11 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre los estándares jurídicos, operativos y técnicos del voto electrónico. Adoptada por el Comité de Ministros del 30 de septiembre de 2004 en su 898ª reunión (original, https://wcd.coe.int/ViewDoc.jsp?id=778189, en castellano en los materiales del curso)

Esta Recomendación, sin exigibilidad jurídica, expresa las normas mínimas que debe contener la regulación de los estados miembros sobre voto electrónico. Se considera que siguiendo sus llamados "principios" y sus "normas de procedimiento" se garantizan los requerimientos democráticos y de los derechos fundamentales. La Recomendación aunque está pensada para el voto electrónico local –el actual-, no excluye su aplicabilidad para el voto a distancia, que reúna las garantías que exige.

La citada resolución recoge como "principios" diversas garantías de estas exigencias ineludibles consagradas en los estados democráticos.

Garantía de voto universal

Se afirman cuatro exigencias:

1º Que el sistema utilizado sea comprensible y fácilmente utilizable por el mayor número de personas posible.

2º Sencillez en el procedimiento para inscribirse y utilizar el sistema de voto electrónico, que no sea una barrera.

3º Que el sistema maximice las posibilidades para los discapacitados.

4º Que mientras no sea universalmente accesible, el e-voto sólo sea un sistema añadido y complementario.

Garantía de voto igual

Se afirman cuatro directrices:

-que se garantice que sólo sea posible un sólo voto electrónico por el elector

- Seguridad de no duplicidad de voto virtual y no virtual.

-Garantía de que el voto se contabilice sólo una vez.

- Que los mecanismos de recuento permitan fácilmente compatibilizar votos electrónico y no electrónico.

Garantía de sufragio libre

- Garantía de identidad (persona real y viva, datos biométricos).
- Garantía de no coacción (en particular para voto a distancia).
- Que la votación electrónica no induzca a un voto concreto, irreflexivo, precipitado o desviado.
- Que sea posible modificación del sentido del voto durante el proceso, sin necesidad de asistencia de un tercero, hasta conclusión del procedimiento de e-voto.
- Posibilidad de no mostrar preferencias, voto en blanco exista también electrónica
- Que el sistema indique con claridad la culminación del proceso con éxito. Mensaje de confirmación y terminación del procedimiento.
- El sistema debe imposibilitar cualquier modificación del sufragio.

Garantía de voto secreto

La garantía del secreto es relativamente sencilla de garantizar en el voto tradicional y en el electrónico local, dada la separación física entre la identificación del votante y la papeleta o el voto electrónico en la urna local (aunque sea electrónica). Por el contrario el secreto es más difícil en el voto a distancia, puesto que debe saberse quién vota (en especial cuando el sufragio es obligatorio), pero no debe saberse su voto. Obviamente es necesario adoptar medidas para que las informaciones requeridas en el tratamiento electrónico no puedan ser utilizadas para violar el secreto del voto.

3. Las "Reglas de procedimiento" del Consejo de Europa

En la Recomendación europea se contienen también un segundo grupo de reglas, relativas a garantías del procedimiento, sobre transparencia (primero), verificación y responsabilidad (segundo) y fiabilidad y seguridad (tercero).

Transparencia

Respecto de la transparencia se exige adoptar siempre medidas para la confianza y comprensión del sistema. Se recomienda que sea posible practicar previamente al voto definitivo. También se exigen medidas que permitan al ciudadano observar el procedimiento electoral electrónico. En este punto se fijan garantías como el conocimiento del programa utilizado –*software*-, medidas físicas y electrónicas de seguridad. En todo caso, la posibilidad de observación debe evitar la posibilidad de manipulación.

Verificación y responsabilidad

Se trata de las cuestiones más discutidas. Se recomienda la divulgación de los componentes del sistema técnico de voto electrónico, al menos a las autoridades electorales competentes, incluyendo información sobre el sistema, código fuente, intentos de intrusión, etc. Asimismo, la Recomendación señala que un organismo independiente debe verificar el sistema de voto regularmente. También, se indica la posibilidad de un segundo recuento de verificación, lo cual tiene muchas variantes (por el mismo sistema, de forma paralela, impresión de papeletas y recuento manual).

Fiabilidad y seguridad

La Recomendación recoge numerosas previsiones, entre las que cabe destacar: verificaciones de seguridad previas al comicio, selección de personal autorizado con accesos al sistema, con sistemas de actuación por parejas –mínimo- y rotación de personal, la incorporación de mecanismos de seguridad a lo largo del procedimiento electoral frente averías y ataques. Mecanismos de encriptación para el caso de salida de la urna electrónica de los datos de los votos, etc.

Para parte de la doctrina, el rastro en papel es "exigencia ineludible", que el resguardo de voto sea depositado en un recipiente: "Cualquier tipo de auditoría posterior de las elecciones realizadas a través de voto electrónico requiere de la constancia impresa." (Martínez Dalmau). Se trata del conocido en términos ingleses como *Voter Verified Papel Audit Trail* (VVPAT)

http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

A mi juicio, esta imposición del rastro de papel puede conllevar la ineficacia del e-voto y la inhibición de todas sus ventajas. Si se da la desconfianza social en el sistema electrónico que lleve a esta exigencia, no debería implantarse un sistema de voto electrónico. Cuestión diferente es el comprobante en papel del voto efectuado o del sentido del voto emitido para la confianza del elector.

4. La duda del voto electrónico nulo

Una de las ventajas del voto electrónico es que excluye la posibilidad de votos nulos, evitando la existencia de un porcentaje pequeño pero indeseable de errores de los electores.

Sobre la base de los principios, si bien debe garantizarse el voto en blanco, parece que no tiene lugar el mantenimiento electrónico del voto nulo. No obstante, la realidad política lleva a que no sea en modo alguno extraño que algunos electores voten voluntariamente de forma nula. Tales mensajes suelen expresar repulsa a la votación, al sistema electoral, al régimen de partidos políticos, desmarcación de posiciones políticas elegidas por otras facciones, etc.

La doctrina no muestra acuerdo sobre el particular, habiendo posiciones en un sentido u otro. Por mi parte, pudiéndose afirmar la existencia en algunos países de una cuarta vía ya casi tradicional de expresión (votar, no votar, votar en blanco y votar nulo), considero que debe mantenerse –por artificial e irracional que resulte- esta posibilidad en el mundo electrónico. Ésta parece ser la opción, por ejemplo, de la Ley 5/1990, de 15 de junio, ley de elecciones vascas reformada por la Ley 15/1998, de 19 de junio de de Elecciones al Parlamento Vasco (art. 132 bis).

5. Las dificultades de control del voto electrónico y la necesaria de confianza social para su implantación

El voto electrónico "plantea, pues, un problema medular, puesto que parece que el voto electrónico impugna la esencia misma de la observación"[2]. Si el escrutinio manual puede hacerlo incluso un analfabeto, el escrutinio electrónico requiere de conocimientos. Señala Jones[3] que con el e-voto se degradan los derechos de los observadores pues "todo lo que el observador puede ver es una caja con algunos ventiladores y luces parpadeantes, y tal vez la espalda del técnico o un programador sentado al teclado que escribe comandos desconocidos en el sistema". Así, con suerte cabe visualizar el proceso, pero no controlarlo. Y esto no es suficiente.

---

[2] BARRAT I ESTEVE, Jordi, "Observación electoral y voto electrónico", en *Revista catalana de dret públic*, nº. 39, 2009 (Ejemplar dedicado a: Els "guardians" de l'autonomia), pags. 277-296, pág. 2 versión electrónica. Texto completo en Dialnet:
http://dialnet.unirioja.es/servlet/articulo?codigo=3100573&orden=242119&info=link

[3] JONES, Douglas W., *The European 2004 Draft E-Voting Standard: Some critical comments*, Iowa City: University of Iowa, 2004, § 56. Disponible en:
http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml

En esta dirección cabe subrayar la reciente sentencia del Tribunal Constitucional Federal alemán de 3 de marzo de 2009 (BVerfG, 2 BvC 3/07)[4] sobre voto electrónico. En la misma se subraya que la transparencia es condición esencial del proceso electoral (§ 106) y que "Cada ciudadano ha de poder seguir y entender de forma fiable las etapas centrales de la elección sin conocimientos técnicos especiales" (§ 109; en el mismo sentido, § 119, 148 y 149). Dicho control real se considera exigible, no bastando que la ingeniería y software hayan sido certificados y auditados previamente (§ 123). El Tribunal exige, entre otras, la publicación de los informes técnicos o el acceso al código fuente (§ 125), lo cual está muy reñido con elementos de seguridad misma y sobre todo, de propiedad industrial. El Alto tribunal estima que ventajas del e-voto como la disminución (o incluso supresión) de los errores involuntarios del elector, que generan votos nulos no deliberados (§ 127), o la rapidez en la publicación de los resultados (§ 130) no constituyen argumentos de peso suficiente como para deshacer la regla común de la publicidad y la comprensión electoral. En el caso enjuiciado se consideran insuficientes las garantías del carácter público de las elecciones (art. 38 en relación con el artículo 20.1 y 20.2 de la Ley Fundamental) ponderadas respecto de los intereses en juego a favor del e-voto.

Una de las posibles ventajas del e-voto es la celeridad del recuento, que no es manual. No obstante, esta ventaja se hace muy relativa en sistemas con listas cerradas y bloqueadas, como suele ser el caso español, en donde el recuento es bastante sencillo y rápido. En el caso español que el sistema electrónico no puede dar la transparencia que aquí se da, pues como se ha visto se cuenta con una potencial y real capacidad de auditar el proceso de escrutinio y recuento por cualquier ciudadano y, sobre todo, por los representantes, partidos y candidatos.

Ahora bien, tampoco hay que cerrar la puerta al e-voto y las ventajas que trae consigo siempre que se consiga la suficiente confianza social. Y es que, todo se hace depender de la confianza ciudadana pues como afirma Barrat "el voto electrónico sería compatible con los principios electorales de cualquier democracia, siempre y cuando las medidas garantistas generaran la suficiente confianza ciudadana"[5]. La confianza es cuestión de adaptación no sólo tecnológica sino, especialmente, social.

En este sentido no parecen muchas las muestras de desconfianza en el voto en países que lo tienen generalizado, como Brasil o India. En Europa, destacan movimientos claramente contrarios al e-voto en Países Bajos

---

[4] El texto en alemán en http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

en inglés, en http://www.bundesverfassungsgericht.de/en/decisions/rs20090303_2bvc000307en.html

[5] Ob cit. pág. 10 versión electrónica.

ONG "No confiamos en las máquinas de votación" (We don´t trust voting computers)

http://www.wijvertrouwenstemcomputersniet.nl

o el Movimiento belga contra el e-voto: http://www.poureva.be/

En Italia se ha llegado a paralizar cualquier avance en la materia bajo la afirmación pública de "Basta con il voto elettronico"

http://www.corriere.it/Primo_Piano/Politica/2006/11_Novembre/29/amato.shtml

Por muy seguro que sea objetivamente un sistema de e-voto, si la desconfianza en la población es también un dato objetivo, el voto electrónico es perverso en sus efectos y condicionar el comportamiento del electorado. Incluso el gobierno puede tener la diabólica conducta de inducir temores sobre el secreto del voto electrónico inhibiendo la votación a favor de la oposición.

Video de Argentina contra el voto electrónico en 10 argumentos por un famoso hacker

http://www.youtube.com/watch?v=7iAgXT8lh10

http://www.youtube.com/watch?v=kizqOsUEATQ&feature=related

Videos –parodia contra el e-voto

Movimiento antibelga:

http://www.youtube.com/watch?v=4g0zbaIQL90

Homer Simpson tries to vote for Obama

http://www.youtube.com/watch?v=1aBaX9GPSaQ&feature=related

6. Ejercicio electrónico formal e informal de iniciativa legislativa popular y del derecho de petición

1. Iniciativa legislativa popular y ejercicio del derecho de petición por vía electrónica

Entre las fórmulas de democracia semi-directa o de democracia participativa (según se conciba), se encuentra la incitación o excitación de los órganos políticos, legislativos y administrativos para que adopten decisiones políticas o normativas. Ello se realiza a través de iniciativas populares u otros mecanismos de participación de la sociedad civil. Las variedades constitucionales y legislativas son muchas tanto por países como en razón de ámbitos de decisión política. Al igual que el derecho de petición, el ejercicio de estas fórmulas según los requisitos, sólo garantiza su tramitación, pero obviamente no el logro del objetivo político o normativo deseado.

El ejercicio electrónico de estas vías democráticas requiere de la conjunción de premisas fácticas, jurídicas y técnicas.

-Por cuanto a las bases materiales, una de las claves para el ejercicio vía electrónica de estas posibilidades se hace depender de la generalización en la población de medios de firma electrónica. Esto en modo alguno está generalizado en América Latina, si bien en España, en marzo de 2010 son más

de 14 millones los DNI electrónicos expedidos. Cuestión diferente es que no muchos sepan o quieran usar estos medios que acreditan la identidad.

-Jurídicamente es necesaria cierta cobertura legal en la regulación de firma electrónica y la específica de iniciativa legislativa o petición. Ha de haber transparencia y seguridad en la comprobación del cumplimiento de requisitos del ejercicio de estos derechos. No obstante, las exigencias no deben ser desproporcionadas para estas finalidades. Del mismo modo, considero que han de adoptarse medidas normativas y de garantía de los ficheros de datos personales de los suscriptores de tales iniciativas, un *botín* político de gran sensibilidad que debe ser jurídica y técnicamente custodiado. En España, la regulación del derecho de petición (Ley orgánica 4/2001, art. 4) menciona su ejercicio electrónico y el antes referido artículo 6 de la Ley 11/2007 garantiza que se puedan formular peticiones de forma electrónica. De otra parte, Ley Orgánica 3/1984 que regula la Iniciativa Legislativa Popular, gracias a su reforma por Ley Orgánica 4/2006, de 26 de mayo), permite recoger firmas para promover cambios legislativos a través de Internet y de medios electrónicos, eso sí, exigiendo firma electrónica (art. 7.4º: "Las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente.").

- Técnicamente, son necesarios sistemas que permitan la recogida de firmas de forma fiable, que sean auditados por las entidades de control. Pues bien, en 28 de enero de 2010 la Junta electoral Central en España ha homologado por primera vez una plataforma de recogida de firmas para presentación de Iniciativa Legislativa desarrollada por una Universidad.

2. Ejercicio informal de iniciativas y peticiones vía electrónica

Hay fenómenos electrónicos de apoyos políticos hasta ahora impensables por cuanto a su magnitud. Quizá el precedente lo encontremos en las campañas de Amnistía Internacional de 2002 para salvar de la lapidación en Nigeria por adulterio a Amina Lawal (luego para Safiya Hussaini), que alcanzaron apoyos millonarios. Desde entonces, han sido muchos los movimientos de "recogida de firmas" o "apoyos" electrónicos informales. Informales por cuanto no se garantiza la verdadera identidad de quien realiza el apoyo o la firma o el número de veces que lo realiza, lo cual, como se ha visto no es muy sencillo. Existen plataformas para el ejercicio informal del derecho de petición o el apoyo a iniciativas (por ejemplo: www.petitiononline.com). Además de sitios donde inscribirse como suscriptor de una iniciativa, una fórmula reciente, por ejemplo, es la del manifiesto electrónico, que supone recoger el texto de un manifiesto en las webs personales o de organizaciones que lo apoyan. Así, por ejemplo, el texto del Manifiesto "En defensa de los derechos fundamentales en internet" de diciembre de 2009 se encuentra en más de 90.000 sitios en la red (http://www.cotino.net/2009/12/manifiesto-en-defensa-de-los-derechos-

fundamentales-en-internet/). Que se trate de un ejercicio informal de derechos no resta el valor político que puedan tener estas iniciativas o movimientos, pero tampoco hay que magnificarlos puesto que la manipulación de los mismos es bien sencilla.

7. TICs, transparencia y acceso a la información pública por el público

1. Principios y derechos de transparencia y acceso a la información pública

La transparencia y el acceso a la información pública han sido objeto de estudio en un módulo anterior.

La Directriz 15 de la Recomendación de e-democracia de 2009 es clara:

"La transparencia en la e-democracia debe incluir la transparencia en el proceso de participación en todos los niveles políticos y en todas las fases de deliberación y en el proceso de toma de decisiones, y durante la ejecución, seguimiento y evaluación."

Las TICs permiten, facilitan y abaratan enormemente esta transparencia. Basta una suscripción a una mera lista de correo para estar informado de cada momento del proceso de toma de decisiones y de las decisiones adoptadas. Sin embargo, como se dijo, hoy por hoy la legislación es bastante renuente y refractaria de imponer obligaciones a los poderes públicos –y derechos a los ciudadanos- en el ámbito de su transparencia e información, obligaciones de empleo de las TICs. Hay mucho desconocimiento y sobre todo, una total falta de compromiso político y jurídico, como es prueba que sí que se exija jurídicamente la "transparencia electrónica" a empresas y sociedades mercantiles.

Las leyes de transparencia son bastante más habituales en América Latina que en España (http://www.bibliojuridica.org/libros/libro.htm?l=1156). En todo caso, en España se ha dado cierto impulso al acceso a la información pública por medios electrónicos con la ya citada Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos. Dicha norma impone la la existencia de "sedes electrónicas" de los poderes públicos con unos contenidos mínimos, impulsa los boletines oficiales electrónicos –cuya versión en papel jurídicamente está desapareciendo; promueve la información institucional de calidad y asegura que el derecho de acceso se pueda ejercer electrónicamente o conocer el estado de procedimiento. No obstante, queda mucho por hacer.

Cabe señalar que la Unión Europea, donde su Carta de derechos fundamentales reconoce el de acceso a la información pública. Y la normativa incluye el pleno acceso de forma electrónica, lo cual viene además exigido por la normativa de desarrollo de este derecho, el Reglamento (CE) n° 1049/2001 del

Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

2. Propuesta de obligaciones jurídicas y derechos de los ciudadanos de acceso a la información pública en la red

En las diferentes legislaciones abundan falsos compromisos y obligaciones no exigibles jurídicamente de implantación de las TICs en favor de la transparencia e información. A continuación, me permito incluir una propuesta de obligaciones y derechos que deben incorporarse bien en las normativas de desarrollo de los mencionados principios y derechos o que, incluso, pueden en casos considerarse obligaciones derivadas del carácter fundamental de algunos derechos en juego, a saber:

-que una institución pública disponga de un sitio web. Esta obligación puede articularse y regularse a partir de parámetros como presupuesto de la institución, número de ciudadanos que componen la población, etc.

-que dicho sitio web cumpla con unas obligaciones de estructura, diseño y servicios.

-que la información de dicho sitio sea accesible (para sectores con dificultades) siguiendo unos estándares reconocidos internacionalmente.

-que la información de dicho sitio sea usable y manejable. Ello se puede obligar jurídicamente estableciendo, por ejemplo, número de "clicks" máximo para alcanzar algunas informaciones temáticas clave u obligando al reenvío a portales temáticos directamente vinculados con la participación y democracia. Con la obligación de disponer de forma sencilla de un mapa del contenido de ese sitio web.

-obligando a la existencia de contenidos mínimos de interés para la participación e información. Por ejemplo:

- la obligación de incluir una serie de contenidos estructurados por temas,
- imposición de temas mínimos para instituciones municipales, provinciales, ministeriales, etc. Según sus competencias jurídicamente reconocidas.
- la normativa básica reguladora de la institución.
- La normativa básica que genera la institución.
- Información sobre las decisiones políticas y normativas en trámite, el procedimiento y posibilidades de participación en las mismas, grupos interesados y posiciones de los actores políticos.

- Información sobre los responsables políticos de la institución, con contenidos mínimos (responsabilidades públicas anteriores, declaración de haberes, resultados electorales, etc.

Steven Clift, por ejemplo, señala para el futuro la necesidad de reconocimiento de unos derechos mínimos como:

-que no pueda darse cualquier reunión pública sin agendas y documentos publicados previamente en la red. "Sin aviso electrónico, no reuniones";

- que toda propuesta legislativa y sus enmiendas fueran accesibles, así como no posible entrar en vigor una norma aprobada no publicada en la red. "Sin transparencia... no autoridad ni dinero".

- derecho ciudadano a ser notificado por correo electrónico sobre información pública basada en el perfil de sus intereses y territorial.

-derecho de acceso sencillo a directorios siempre actualizados y locales de "mi democracia", con datos de contactos de todo cargo público elegido. "Ningún dato de contacto, ningún poder".

Como puede observarse, la propuesta hacer referencia a entes y órganos públicos, entre los cuales, obviamente puede considerarse los parlamentos o órganos representativos de que se trate, al igual que si se trata de entes de naturaleza gubernamental o administrativa.

3. Calidad de la información pública y mecanismos de control de la transparencia

Estas obligaciones para los poderes públicos hoy día extrañamente son reconocidas –sólo en algunas leyes de administración electrónica de países avanzados-, pese a la paradoja de que se están imponiendo a particulares Es factible que en unos años, estas pretensiones se consideren jurídicamente integrantes de derechos de los ciudadanos.

El proceso de reconocimiento será, posiblemente, sectorial (procedimientos administrativos en masa: medio ambiente, urbanismo, planificación, etc.) y gradual.

Hay que advertir que una mayor información no implica un público más y mejor informado. La saturación de información, la manipulación o el control sobre la misma, la falta de posibilidades, la falta de calidad de la información o de estímulos para que la información se torne conocimiento llevan correr el peligro de peor información y ciudadanos peor informados. Además, es el emisor quien selecciona la información y la hace más o menos accesible en parámetros materiales (difícil de controlar jurídicamente) con todas las consecuencias que ello entraña.

Es por ello que se consolidan conceptos no difíciles de trasladar al ámbito jurídico, como acceso y accesibilidad a la información, como los propuestos por el G-8:

"Acceso significa la posibilidad real de consultar o acceder electrónicamente a la información.

Accesibilidad significa la facilidad con la que uno puede hacer uso real de la posibilidad de acceder a la información electrónica."

Y son diversos los parámetros que sirven para fijar el grado de accesibilidad a la información pública electrónica, a saber: Recognoscibilidad y localizabilidad; disponibilidad; manejabilidad; Precio razonable (*affordability*); responsabilidad y confianza; claridad; accesibilidad para los limitados.

Jurídicamente debe subrayarse la responsabilidad patrimonial de los poderes públicos por la información propia que difundan en sus sitios. Aunque incluyan cláusulas de exención de responsabilidad por la calidad de sus contenidos, el alcance de éstas ha de ser muy relativo. En todo caso, habrá que estar a la regulación concreta de la responsabilidad patriminonial en cada país.

Los principios expuestos deben aceptarse como criterios inspiradores de toda actuación de información pública por la red. Y el control de la regulación y el cumplimiento estos principios puede ser responsabilidad de distintas instituciones. En ocasiones hay instituciones específicas para velar por el acceso a la información pública, como el Instituto Federal de Acceso a la Información Pública (IFAI) en México (www.ifai.org.mx/) en razón de su avanzada ley de transparencia de 2003. En algunos países se sigue el modelo anglosajón por el que la autoridad independiente que controla la protección de datos personales, controla también el acceso a la información pública. En países donde desde hace lustros existen agencias de protección de datos con una fuerte inercia hacia su protección frente a la transparencia, este modelo puede ser negativo para el acceso a la información público. También, diversas instituciones pueden pasar a responsabilizarse del cumplimiento de normativa de transparencia, como las mismas defensorías del pueblo o comisionados ya existentes en diversos países del mundo anglosajón (*Information Commissioner* o *Information Tribune*).

Cuestionario Sobre democracia electrónica

Cita tres formas de nombrar el fenómeno de la e-democracia o democracia electrónica entre su variada terminología.

Qué quiere decirse con la "versión fuerte" y "débil"? ¿Cuál crees que es la más adecuada para el autor del texto?

Crees que el concepto de gobierno electrónico tiene algo que ver con e-democracia?

Cita 5 ventajas se alegan básicamente para el e-democracia y e-gobierno?
1
2
3
4
5

Crees que hay una clara obligación constitucional de implantar la e-democracia? ¿A quién correspondería la concreción de una obligación constitucional?

¿Es posible traducir en obligaciones concretas las exigencias de e-democracia? ¿Se te ocurre cómo?

¿Qué ejemplo de hipocresía en la regulación cita el autor?

Crees que el voto electrónico en entorno controlado puede cambiar el sistema político, por qué?

En qué países es habitual este tipo de voto?

Qué problemas presenta el voto telemático?

Qué se dice de la exigencia de firma electrónica para las iniciativas legislativas?

IV. LIBERTADES Y RESPONSABILIDAD EN LA RED

1. A modo de introducción: Libertades informativas y su difícil adaptación a internet, Lorenzo Cotino

Son ya muy diversos fenómenos comunicativos a través de la red y alternativos a los medios de comunicación tradicionales –como los *blogs*- o la expresión de movimientos sociales a través de la red. Curiosamente, la mayoría de las aproximaciones a la democracia electrónica, desatienden estos fenómenos de nuevas formas de ejercicio de las libertades de expresión de información, siendo que superan y con mucho en importancia a las acciones públicas de democracia y participación electrónicas.

Tipología de modos y medios de comunicación en internet

es útil hacer una relación de algunos de los nuevos modos y medios de comunicación en internet.

Internet como canal de comunicación interpersonal:

1. correo electrónico,
2. listas de distribución,
3. grupos de noticias,
4. chats,
5. redes P2P (*peer to peer*),
6. foros de debate,
7. wikis, ejemplo wikipedia
8. juegos en red,
9. encuestas,
10. comunidades virtuales.

Internet como medio de comunicación de masas:

1. Páginas personales y páginas de asociaciones, instituciones y empresas,
2. weblogs o blogs, páginas personales de autor sobre temas diversos y posibilidad de colaboración por usuarios.
3. portales temáticos,
4. buscadores y directorios (como *Google* o *Yahoo*).

5. Dentro de estos medios de comunicación a través de internet, hay que hacer referencia al llamado "Ciberperiodismo". Y dentro de este periodismo digital se puede distinguir entre:

-*los medios tradicionales en internet:*

-*A diferencia de los medios tradicionales, pueden distinguirse los medios alternativos.* En este heterogéneo grupo, podemos fijar fenómenos relativamente nuevos:

a) periódicos "confidenciales"

b) prensa fuertemente ideologizada, relativamente similar a los antiguos panfletos, pasquines y antiguas radios libres.

c) nuevos fenómenos como el periodismo "open source", fuente abierta, como 20minutos y, en especial, fenómenos como el periódico koreano www.ohmynews.com (con más de 37.000 "periodistas" ciudadanos que aportan unas 200 noticias diarias, un 70% del total que produce OhMyNews).

d) por último, dentro del periodismo digital, cabe mencionar los selectores y reproductores de información ajena como Google news y el fenómeno del *press clipping.*

Asimismo, cabe ya anunciar que existe una revolución en el mundo del periodismo, especialmente intensa en Estados Unidos. A Europa y Latinoamérica también han llegado sus efectos, pero no de forma tan significativa. Uno de los causantes fundamentales de esta revolución es el fenómeno de los *weblogs o blogs*. De hecho, en norteamérica hay una guerra en internet (medios clásicos y medios alternativos) y el Derecho va a ser un elemento muy importante para decidir esa guerra y para configurar el futuro de internet y de los medios de comunicación. Las últimas sentencias parece que inclinan la balanza a favor de los nuevos medios en internet.

La libertad de expresión e información protege en general internet y a todos los internautas

Internet está protegido por la libertad de expresión. Así se asentó en el importante caso ACLU vs Reno de 1997, el Tribunal Supremo de los EEUU reconoció para internet la libertad de expresión, con un nivel de protección semejante a la prensa escrita, es decir, una libertad de expresión menos limitada que la radio o la televisión.

Creo que como primera consecuencia, hay que afirmar que sería contrario a la libertad de expresión exigir una autorización previa para la presencia en la red o someterlo a los requisitos del servicio público.

De otra parte, con internet todos podemos emitir y recibir información de forma mucho más sencilla, sin necesidad de acceder a los medios de comunicación social clásicos. Ello lleva a que todas las expresiones e informaciones estén amparadas, sin necesidad de ser periodistas. La libertad de expresión e información es un derecho de todos, no sólo de los periodistas. Así Tribunal Supremo de Estados Unidos, en el caso Branzburg v. Hayes de 29 de junio de 1972, dijo que "la libertad de la prensa es el derecho de un solo panfleto... al igual que el de la más importante publicación metropolitana". La sentencia Engels del TEDH, de 8 de junio de 1976 afirmó que "Está

claro que la libertad de expresión garantizada por el artículo 10 es aplicable a todas las personas" (& 100).

En todo caso, internet es como la calle, donde podemos hacer uso de nuestras libertades, pero no todo es libertad de expresión e información en internet. Determinar cuándo se ejerce o no la libertad y se adquiere la protección especial de los derechos fundamentales no siempre será sencillo.

En todo caso, finalidad del libre flujo de la opinión e información, la relevancia pública del mensaje, serán los elementos básicos para el juicio sobre la intensidad de la protección constitucional. Los mensajes comerciales y los no propiamente políticos en muchos casos también deben considerarse ejercicio de estas libertades, aunque no merezcan una protección reforzada por su relevancia pública.

En teoría, que la libertad de expresión e información se ejerza o no por medios de comunicación clásicos en internet, o en otros ámbitos, no debe hacer variar su tratamiento jurídico.

Anonimato en la navegación y uso participativo de internet

Afirma Lessig que lo predeterminado en la red es el anonimato[6] o así lo ha sido hasta la fecha. Nadie duda de que el secreto es una precondición de libertad para el ejercicio del voto. Sin embargo, no se afronta el anonimato desde la libertad, en general la libertad de expresión, cuando sociológica y psicológicamente es obvia la sensación de libertad que otorga el anonimato en la red[7]. Con Roig Batalla en su brillante

6 En este sentido, recuerda Lessig que:

"en el ciberespacio ocultar quién eres o, más exactamente, tus características identificadoras es la cosa más sencilla del mundo. La condición predeterminada en el ciberespacio es la anonimidad. Y al ser tan fácil ocultar quién es uno, es prácticamente imposible que las leyes y las normas se apliquen en el ciberespacio. Para que estas leyes se apliquen, uno tiene que saber que la persona con la que está tratando es un menor. Pero la arquitectura del ciberespacio, simplemente, no ofrece esa información."

LESSIG, Lawrence, "Las leyes del ciberespacio", en *Cuadernos Ciberespacio y Sociedad* Nº 3, Marzo 1999 (trad. Javier Villate), del original en: cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (3 abril 1998) Dispuesto para su acceso en http://cys.derecho.org/03/leyes.html (2/5/2005).

7 Como señala Wolton, Internet genera consecuencias psicológicas relativas a la sensación de apertura y de liberación antropológica. "Las dimensiones psicológicas son esenciales en la atracción por las nuevas tecnologías, ya que éstas reúnen el profundo movimiento de individualización de nuestra sociedad" "cada uno puede actuar sin intermediario cuando quiera, sin filtros ni jerarquías y, lo más importante, en tiempo real,... "un sentimiento de libertad absoluta, incluso poder" ejemplificado en la expresión "navegar por la red", WOLTON, Dominique, *Sobrevivir a Internet. Conversaciones con Olivier Jay*, Gedisa (Colección : El Mamífero parlante), Barcelona, 2000, pág. 95. Cito por FERNÁNDEZ RODRÍGUEZ, José Julio, *Lo público y lo privado en internet. Intimidad y libertad de expresión en la red,* UNAM, Instituto de Investigaciones Jurídicas, Méjico, 2004, pág. 192.

trabajo[8], hay que apostar por este enfoque, salvo excepciones más bien simbólicas poco habitual en el marco europeo[9]. A diferencia de los Estados Unidos, aquí se aborda la cuestión desde la vida privada, secreto de telecomunicaciones y protección de datos. Allí, el análisis del anonimato queda desde antiguo vinculado a la libre expresión[10], afirmándose más recientemente, en McIntyre v. Ohio Elections Comm'n (1995)[11] que:

"De acuerdo con nuestra Constitución el panfleto anónimo no es una práctica fraudulenta y perniciosa, sino una honorable tradición de argumentación y disentimiento. El anonimato es el escudo frente a la tiranía de la mayoría".

Y esta doctrina se ha trasladado recientemente para internet en el caso en Delaware John Doe nº1 v. Cahill[12], donde se apunta que el anonimato no es ilimitado frente a la difamación, pero se acude a un canon estricto en su protección, por lo que, de un lado, hay que descartar recursos por motivos triviales o nimios para revelar la identidad y, de otro, hay que atender al contexto[13].

A mi juicio, cabe esperar cierta traslación de estos principios en nuestro marco jurídico, puesto que el derecho permite este tipo de ponderación entre el interés de perseguir y evitar conductas ilícitas y la preservación de marcos que facilitan la libre

---

Sobre el tema en general, BARRAT I ESTEVE, Jordi, "El Anonimato como Parámetro Normativo de la Sociedad de la Información" Journal Informática y Sociedad. Vol. 1 No.2 (2004), pág.. 30-33, http://www.itba.edu.ar/capis/jis/index.htm. También, MORÓN LERMA, Esther, *Internet y Derecho penal: Hacking y otras Conductas Ilícitas en la Red*, Aranzadi-Thomson, (2ª ed.), Pamplona, 2002, pág. 99 y STALLABRASS, J. "Formas de la identidad en el ciberespacio", *Revista de Occidente,* nº 206, 1998, pág. 80.

8 ROIG BATALLA, Antonio, "El anonimato y los límites a la libertad en internet"en COTINO HUESO, Lorenzo (Coord.), *Libertad en internet. La red y las libertades de expresión e información,* cit.

9 En el marco del Consejo de Europa, algún documento sin valor jurídico ha conectado expresamente el anonimato con la libertad de comunicación en internet. Así la Recomendación nº R(99)5 del Comité de Ministros de los Estados miembros del Consejo de Europa sobre la protección de la intimidad en Internet se afirma "la necesidad de desarrollar técnicas que garanticen el anonimato de las personas afectadas y de la confidencialidad de la información intercambiada a través de las "autopistas de la información", en el respeto de los derechos y libertades de los demás y de los valores de una sociedad democrática". Más recientemente, la Declaración del Comité de Ministros del Consejo de Europa, de 28 de mayo de 2003, sobre la libertad de comunicación en Internet, Principio 7: Anonimato.

10 Siguiendo el trabajo de Roig Batalla, cabe recordar que , desde el caso del Tribunal Supremo de 1960, Talley v. California se da esta conexión. El Tribunal Supremo americano recurre a la importancia histórica del anonimato recordando *El Federalista* de los padres fundadores, afirmando que en momentos y circunstancias no se puede obligar a ciertas personas a identificarse públicamente.

11 McINTYRE v. Ohio Elections Comm'n, 514 U.S. 334 (1995), se decidió que procede aplicar el "exacting scrutiny" y considera, pues, que la existencia de un interés general público permite el anonimato.

12. John Doe nº1 v. Cahill, 2005, WL 2455266 (Del., October 5, 2005), disponible en http://internetcases.com/library/cases/2005-10-05-cahill_v_doe.html, última visita 06-02-2006. El nombre John Doe es usual en los casos americanos para designar a un individuo que quiere mantener el anonimato.

13. También en DENDRITE v. DOE, 775 A.2d 756 (NJ. Super Ct. App. Div. 2001), el Tribunal de Apelaciones de Nueva Jersey elaboró un test reforzado.

participación del ciudadano en la red. A continuación se relacionan dos cuestiones vinculadas con la cuestión.

No cabe una mayor limitación en internet

En internet deben aplicarse las normas y los límites de la libertad de expresión e información, está claro, pero no deben aplicarse mayores límites que a otros medios de comunicación. Es más, en Estados Unidos se ha dicho que el estándar de limitación ha de ser el mínimo en internet, como el de la prensa.

Sin embargo, no es extraño que para internet aparentemente se expresen mayores posibilidades de límites en las normas y lo que es más importante, que se generen mecanismos de control público de los contenidos que no se dan para la prensa tradicional. Hay que estar alerta frente a estas situaciones.

Estos tratamientos diferenciados para internet no son automáticamente constitucionales, pero pueden serlo por su efecto disuasorio para la libertad en la red (el llamado *chilling effect* aplicado por el Tribunal Supremo EEUU en la ya clásica sentencia de 1997).

De igual modo, dependiendo del país, es dudosa la posibilidad de que las autoridades administrativas puedan controlar y retirar contenidos de la red en ejercicio de la libertad de expresión e información, e incluso sancionar por tales contenidos. Se trata de una cuestión polémica no resuelta hoy día. La sola amenaza de la aplicación de estas leyes de control no judicial pueden ser, en su caso, consideradas inconstitucionales.

La garantía de que sólo un juez pueda decretar la medida del secuestro de los soportes del mensaje u opinión, parece, hoy por hoy, difícilmente trasladable a la red, puesto que se trata de soportes "materiales".

Pluralismo en internet y posible "censura" por empresas privadas

En principio, la facilidad de estar presente en la red es muy grande, sin muchos medios o recursos. Ello facilita la pluralidad en la red. Cuestión muy diferente es ser "visible" en la red. Encontrar contenidos en más de 4 billones de páginas web puede ser peor que encontrar una aguja en un pajar. Para ello hay medios privados que facilitan el acceso a la información, como Google o Yahoo. Estar presente entre los primeros resultados de estos medios es garantía de visibilidad en la red.

Afortunadamente los criterios de visibilidad en estos buscadores son bastante "democráticos" (popularidad en la red por otros internautas, enlaces que desde otras páginas llevan a la página y actualización de contenidos). En todo caso, se trata de empresas privadas que pueden, en principio, hacer lo que quieran, incluso "censurar" a quien quieran en sus buscadores.

Hay que decir que la categoría de "censura" sólo se reserva para los poderes públicos, y en este caso se trata de autocensura.

Considero que las empresas privadas también pueden cometer una lesión de un derecho fundamental, como el caso de que instrumentos tan importantes censurasen políticamente contenidos. El Derecho hasta ahora no da una respuesta, pero considero

que el interés público podría justificar una actuación legislativa que impusiese a tales buscadores no utilizar criterios políticos para omitir resultados de búsqueda y, en todo caso, hacer públicos todos los criterios que pueden servir para restringir políticamente resultados.

Proyección de algunas categorías y garantías de las libertades informativas a internet

Una clave: la relevancia o interés público de la noticia

Considerar el "interés público" y la "necesidad para la formación de la opinión pública" de una información es clara: hace más intensa la protección de la información al rebajar la protección de otros derechos y bienes constitucionales con los que colisiona. Cualquier información u opinión en internet por cualquier persona puede tener esta protección.

Para considerar la existencia de este interés, relevancia y necesidad, son muchos los parámetros jurídicos elaborados (importancia objetiva de la noticia –naturaleza del hecho u acontecimiento del que se informa, actualidad-, importancia y naturaleza subjetiva de los afectados –cargos históricos, cargos públicos, "famosos", etc. la actividad desarrollada por éstos-, el contexto, etc.). Cabe también recordar que jurídicamente el interés público de la información es un concepto diferente del interés *del* público o curiosidad por dicha información. Asimismo y hasta ahora, el interés público de una información es un concepto objetivo que no viene determinado porque la información haya sido objeto de publicación por un medio de comunicación.

En general, los tribunales no han querido ser severos y restrictivos en la consideración de si una información no era objetivamente de interés público. Es muy posible que hasta ahora los tribunales implícitamente considerasen que la información tenía interés público sólo por el hecho de que la noticia se recogiera en los medios tradicionales. Los medios de comunicación clásicos eran un filtro *material* –no jurídico- para determinar qué información gozaba de interés público

Sin embargo, con la sociedad de la información, los nuevos modos de comunicación de internet multiplican exponencialmente la información que se genera, ya no existe ese filtro material de los medios de comunicación clásicos que daba "pistas" a los jueces de a qué informaciones había que dotarles de una mayor protección por ser de interés público y contribuir a formar la opinión pública.

La veracidad y la diligencia del informador y el derecho de réplica o rectificación

Como sabemos, hay libertad de información y de prensa sobre hechos verdaderos, en el sentido de que el periodista haya sido más o menos diligente en su labor. Es muy posible que poco a poco esta exigencia de veracidad y diligencia de la información tenga que adecuarse a un entorno muy distinto del de la profesión periodística clásica.

No es necesario ser profesional para producir información y opinión en internet, pero la diligencia debe de mantenerse. Para ello puede resultar útil el ejercicio del

derecho de rectificación o de réplica ante cualquier información incorrecta en un modo o medio de comunicación en internet.

La aplicación de este derecho se ha reconocido en Estados Unidos en 2003 (Georgia Supreme Court: Georgia rMathis v. Cannon.) o recientemente en España (Audiencia Provincial de Asturias, de Asturias (Sección 6ª) de 3 de junio de 2002, para un foro) exigiendo un juez la rectificación en lo afirmado en un foro de internet, aunque lo cierto es que sentencias más recientes han negado este derecho para internet por no ser un "medio de comunicación" (caso foro leonés).

Lo cierto, en todo caso, es que hoy día es casi imposible controlar la diligencia de la información en internet. En la red los contenidos se multiplican y reproducen de un sitio a otro a veces de forma automática, muchos contenidos –y por supuesto los más polémicos-, se aportan anónimamente en la mayoría de los sitios web. Asimismo, no hay que olvidar que los servidores no tienen ni posibilidad ni obligación legal de controlar la licitud de los contenidos que introducen en las páginas web de las que son responsables técnicos, pero no editores.

Pese al mantenimiento jurídico de las exigencias de diligencia, y la misma protección de la intimidad o el honor, las posibilidades de acción real se reducen. Es muy posible que haya que reconsiderar jurídicamente estas actuales exigencias.

El secreto profesional del periodista en internet ¿para todos?

Como se ha dicho, todos somos "periodistas" en internet cuando generamos contenidos, pero está claro que no todos son profesionales. En muchas constituciones el privilegio del derecho a no revelar las fuentes de información se reserva a los profesionales, en otras ocasiones, a los "periodistas".

Lo cierto es que la trascendencia de internet en países como Estados Unidos ha llevado a que muchos particulares tengan a través de sus páginas personales o *blogs*, una trascendencia mucho mayor que los periodistas profesionales. La importancia de la cuestión es mucha, puesto que muchos de los más importantes blogs garantizan el anonimato en internet a quienes les remiten información, muchas veces ilícitas.

Ver el foro www.drudgerepport.com (con más de 300 millones de visitas al mes).

Por ello, ya en 2004 comenzaron a conseguir acreditaciones como periodistas profesionales, como en las elecciones Bush vs. Kerry. Asimismo, desde 2005 los tribunales de Estados Unidos (juez de Santa Clara, marzo 2005, Caso Apple y Dan Gillmore - de forma más clara en la Corte Estatal de Apelaciones de San José en mayo de 2006-, y en caso John Doe nº1 v. Cahill, de octubre de 2005, en Delaware). Los efectos de este tipo de resoluciones pueden ser decisivos para el futuro de internet, vista la experiencia de los *blogs* en Estados Unidos.

Buscadores, AEPD desde perspectiva de libertades

Declaración sobre buscadores de Internet
Agencia Española de Protección de Datos
1 de Diciembre de 2007
4.3 La legitimación para tratar datos de terceros

La licitud o no de esta difusión de la información puede fundarse en circunstancias muy diversas, por ejemplo, el ejercicio de los derechos fundamentales vinculados a la libertad de información; el cumplimiento de obligaciones legales que exigen la difusión, inclusive por medios electrónicos de la misma, el consentimiento inequívoco de los afectados y otras. En la medida que los buscadores en Internet se limitan a indexar esta información, la legitimación para su tratamiento sería responsabilidad, en origen, de quienes permiten el acceso a la misma.

Si bien no pueden olvidarse dos circunstancias:

- Que los buscadores en Internet llevan a cabo un tratamiento de la información propio y diferenciado de los "sitios web", cuyo acceso facilitan.

- Que la legitimación para el tratamiento de datos personales de quienes hacen accesible la información personal no se extrapola, en todos los casos, a los servicios de búsqueda que facilitan el acceso a ella.

En el caso de los buscadores de Internet la legitimación propia de quienes prestan este servicio puede encontrarse inicialmente en la LSSI. Como se desprende de su Exposición de Motivos esta norma pretende establecer un marco jurídico adecuado que genere en todos los actores intervinientes en Internet "la confianza necesaria para el empleo de este nuevo medio".

La provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet se califica en la LSSI como un servicio de intermediación. La Ley reconoce un interés legítimo en orden a la prestación del servicio excluyendo inicialmente su responsabilidad por la información a la que dirijan a los destinatarios de sus servicios. Si bien, les impone un deber de colaboración "para impedir que determinados servicios o contenidos ilícitos se sigan divulgando", como puede suceder cuando se lesionan los derechos que la LOPD reconoce.

De esta conclusión pueden desprenderse varias consecuencias: Que la legitimación para el tratamiento de datos personales que realizan los buscadores en Internet puede ser cuestionada por los déficits de información que se han expuesto; que, por ello, es urgente analizar nuevos mecanismos informativos que permitan a los usuarios conocer efectivamente el uso de sus datos personales y que es preciso aproximar las diversas políticas de privacidad de los buscadores para que, permitiendo la prestación de los servicios de búsqueda, minimicen las consecuencias para la privacidad de los usuarios.

7. Garantizar los derechos a los usuarios y a terceros.

La LOPD ha venido a dotar a los ciudadanos de esos instrumentos de reacción, fundamentalmente a través de los derechos de cancelación de los datos y de oposición a su tratamiento, que tienen como objeto que éste no se lleve a cabo o se cese en el mismo.

La AEPD ha ido delimitando a través de diversas resoluciones4 criterios para tutelar el derecho de cancelación respecto de la información disponible en Internet y, específicamente, la procedencia del derecho de oposición en servicios de búsqueda (5 TD/00463/2007)

CONCLUSIONES

6- Es urgente desarrollar nuevos mecanismos informativos, claros y suficientemente visibles que permitan a los usuarios conocer efectivamente el uso de sus datos personales cuando utilizan los servicios de los buscadores.

8- Los servicios de búsqueda están obligados a respetar los derechos de cancelación y oposición de personas cuyos datos se indexan desde otras páginas web en su función de buscador.

Aunque la incorporación inicial de esta información personal a la red pueda estar legitimada en origen, su mantenimiento universal en Internet puede resultar desproporcionado.

Libertad de expresión y derecho de oposición de datos ante medios o webs
Caso google, caso foro

"Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal".

Como se acaba de señalar la Ley prevé la inserción de la notificación en el Diario Oficial en los términos ya expuestos.

Pero la Ley no dispone que los datos personales del reclamante figuren en los índices que utiliza Google para facilitar al usuario el acceso a determinadas páginas, ni tampoco dispone que figuren en las páginas que Google conserva temporalmente en memoria "caché".

No existe, por tanto, una disposición legal en contrario respecto del ejercicio del derecho de oposición frente a Google.

ESTIMAR la reclamación formulada y el derecho de oposición ejercido por **Don X.X.X.** contra **GOOGLE SPAIN, S.L.,** instando a Google a que adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos.

Sistema de ida y vuelta de retirada de contenidos de la Digital millenium

Conocimiento de los ilícitos por parte de los PSSI

En los EE. UU., el *Digital Millennium Copyright Act* (*DMCA*, aprobado en octubre de 1998) establece, para el marco del *copyright* ("Derecho de Autor" anglosajón) que un proveedor de espacio **no incurre en responsabilidad cuando elimine** material que infrinja presuntamente el Derecho de Autor

- si ha tenido **conocimiento** de dicha infracción en virtud de una notificación que reúna ciertos requisitos formales —incluyendo la firma electrónica del denunciante y una clara identificación del mismo y del material infractor, con los datos necesarios para ponerse en contacto y una promesa de actuar de buena fe, entre otras exigencias— y se haya dirigido a los destinatarios que marca la norma (y que son los que haya previsto el proveedor de espacio para tales notificaciones).

Además, **una vez eliminados dichos materiales, el proveedor debe informar** lo antes posible de su retirada **al titular del sitio** donde estaban o a quien fuere responsable de los mismos con el fin de evitar incurrir en responsabilidad por su parte (recoge, aun sin mención expresa, la llamada defensa del "buen samaritano", según citan los antecedentes del propio *DMCA*,; en los EE. UU. se hace referencia a la defensa o inmunidad del "buen samaritano", que es la que puede oponer quien causa algún daño cumpliendo sus obligaciones o, incluso, realizando "buenas acciones" que no tenía obligación legal de hacer).

Si titular éste mantiene que los está utilizando legítimamente, el proveedor vendrá obligado nuevamente a activar el acceso al sitio, quedando eximido de responsabilidad tanto por la posible ilicitud de los contenidos (frente a su presunto titular) como por la retirada de los mismos que llevó a cabo (frente a quien contrató sus servicios).

No obstante, **si quien notificó la presunta infracción presenta demanda** ante los Tribunales frente al infractor, el proveedor de espacio **deberá retirar nuevamente** el material **a la espera de lo que decida el órgano jurisdiccional**. La sucesiva trasgresión de estos deberes del proveedor en relación a cada una de las notificaciones y contranotificaciones efectuadas originará la correspondiente responsabilidad. Todo el procedimiento de notificación y retirada y la responsabilidad del proveedor de servicios aparecen reguladas en la sección 512 del *Copyright Act*, tras las modificaciones introducidas por el DMCA.

2. Algunas posiciones muy críticas o "libertarias" a la regulación de la red, en concreto en España (www.lssice.com)

Javier A. Maestre es abogado y dirige actualmente dominiuris.com, desde su creación en 1997. Es autor del libro que acaba de publicar con el título "El Derecho al Nombre de Dominio".

Carlos Sánchez Almeida es abogado y socio fundador de Bufet Almeida, Advocats Associats (www.bufetalmeida.com) y autor del libro "Todo está en venta.

Globalización, Internet y Derechos Humanos", que puede descargarse libremente desde Internet.

No pasarán: Fascismo digital

http://www.lssice.com/textos/fascismo.html
Carlos Sánchez Almeida
almeida@kriptopolis.com
Abogado

"Dejando aparte las siglas y el argot que han sembrado la vista, Internet puede muy bien ser descrita como una conversación universal sin fin. El Gobierno no puede, a través de la Ley de Decencia en las Telecomunicaciones, interrumpir esa conversación. Como la forma participativa de expresión de masas más desarrollada jamás conocida, Internet merece la más estricta protección frente a la intrusión gubernamental. Es cierto que muchos encuentran algunas de las expresiones o manifestaciones en Internet ofensivas y es cierto, también, que, en medio del estruendo del ciberespacio, muchos oyen voces que consideran indecentes. La ausencia de regulación gubernativa de los contenidos de Internet ha producido, incuestionablemente, una especie de caos, pero, como uno de los expertos propuestos por los demandantes indicó en el curso de la vista, lo que ha hecho de Internet un éxito es el caos que representa. La fuerza de Internet es ese caos. Como sea que la fuerza de Internet es el caos, la fuerza de nuestra libertad depende del caos y de la cacofonía de la expresión sin trabas que protege la Primera Enmienda. Por estas razones, sin dudarlo, considero que la Ley de Decencia en las Comunicaciones es "prima facie" inconstitucional y concedo las medidas cautelares solicitadas."

Sentencia de la Corte del Distrito Este de Pensilvania, en el caso entre la American Civil Liberties Union versus Janet Reno, Fiscal General de los Estados Unidos.

Por encargo de la Asociación Europea de Abogados Jóvenes, la pasada semana me vi en la obligación de exponer una ponencia ante su Asamblea General, celebrada en el Colegio de Abogados de Barcelona, bajo el título "Internet y comercio electrónico en España". Dado que no disponía de mucho tiempo, decidí ofrecer a nuestros colegas europeos una visión general de la situación actual, dejando para el final las perspectivas de futuro, encarnadas en el Anteproyecto de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. Nunca pensé que lo iba a pasar tan mal, ni que podría acabar tan avergonzado de ser español. Después de estudiarme el proyecto legislativo, decidí que nuestros colegas tendrían que volver a sus respectivos países explicando que en España iba a aprobarse por ley la implantación de censura previa en Internet.

Cuando hace pocas semanas un responsable gubernamental explicaba que el texto legislativo prohibiría el SPAM, ya comencé a pensar que había gato encerrado. Efectivamente, la presunta ilegalización del SPAM no era más que el cebo para que la comunidad internauta pasase de puntillas sobre el texto de la Ley. Una ley que pretende, ni más ni menos, suprimir por vía legislativa la existencia de comunidades libres en la Internet española, eliminando de un plumazo el anonimato, la discrepancia y la libertad de expresión. Una ley que pretende destruir nuestra Ciudad Oculta.

El anexo de la Ley establece que se entenderá como "servicio de la sociedad de la información", además del comercio electrónico, todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, incluyendo, entre otros servicios, el suministro de información por vía telemática. En lenguaje internauta, cualquier revista online financiada mediante banners, como Kriptópolis.

En el artículo 9 se establece que los prestadores de servicios deberán comunicar a un Registro Público el nombre de dominio e internet que utilicen con carácter permanente. De Network Solutions a la matrícula obligatoria de nombres de dominio: vamos progresando, Birulés.

En el artículo 10 se establece que estarán obligados a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos administrativos o judiciales competentes, acceder de forma permanente, fácil, directa y gratuita a toda la siguiente información: su nombre o denominación social; su domicilio social o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva. Manolo Gómez, con el carnet en la boca.

En el artículo 11 se establece que todos los prestadores de los servicios de la sociedad de la información deberán convertirse en ciberpolicías, puesto que en caso contrario podrían ser multados hasta en 100 millones de pesetas. Las obligaciones para Kriptópolis y cualquier otra revista online son las siguientes:

a) Comunicar a las autoridades judiciales o administrativas competentes, tan pronto como tengan conocimiento de su existencia, la actividad presuntamente ilícita, realizada por el destinatario del servicio.

b) Comunicar a las autoridades judiciales o administrativas competentes, a solicitud de éstas, la información que les permita identificar a los destinatarios de servicios.

c) Suspender la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio de la sociedad de la información, en ejecución de resoluciones dictadas por una autoridad judicial o administrativa.

d) Cuando así les sea requerido por una autoridad judicial competente, supervisar o conservar todos los datos relativos a la actividad de un determinado destinatario durante un período máximo de seis meses y ponerlos a su disposición.

Los artículos comentados establecen de hecho el fin de Internet concebida como un espacio libre. Al convertir el suministro de información en una actividad económica regulada, la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico pretende acabar con publicaciones como Kriptópolis. Publicaciones basadas en economía de subsistencia -pero economía al fin y al cabo: a ver cómo, si no, se sirven cientos de miles de páginas a decenas de miles de suscriptores- y en consecuencia sometidas al cepo administrativo. Un cepo que pretende amordazar la libertad de expresión, obligando a las revistas independientes a suspender la transmisión de información cuando les sea requerido por una autoridad administrativa, algo que no pasaba en España desde la aprobación de la Constitución.

Decíamos hace pocas semanas que estabamos tocándoles mucho las partes nobles a un par de virreyes, y que antes o después querrían vengarse. Ahí lo tienen. Impedir

que se espíe a los trabajadores y denunciar la subordinación del poder político a los intereses de las grandes corporaciones y sus grupos mediáticos, tiene su precio.

Lo que no consiguieron a golpe de talonario, lo pretenden ahora por la vía del decreto ley. Pretender que la publicación de una noticia, o la opinión discrepante de un internauta, pueda ser sometida a censura sin intervención de un juez, sólo tiene un nombre: fascismo digital. Llevamos luchando mucho tiempo por una Red libre, y quizás éste sea nuestro último combate, pero al menos ahora ya sabemos a qué nos enfrentamos.

A las armas digitales, ciudadanos: no pasarán.

Por Javier A. Maestre

maestre@dominiuris.com
Abogado

La iniciativa que desarrolla Kriptópolis, poniendo de manifiesto los espurios intereses y objetivos que se esconden tras el texto llamado a ser la Ley de Servicios de la Sociedad de la Información, sin duda, es llamativa y, ciertamente, acertada y oportuna.

Pero, ¿por qué tanto alboroto y por qué denominarla la tercera guerra mundial? Pues porque este proyecto de texto legal es una de las muestras del tercer pulso que los titulares del poder anterior a Internet le echan a sus indígenas; las dos primeras guerras las perdieron y, a menos que se reaccione a tiempo, corremos grave riesgo de que a la tercera vaya la vencida.

La primera guerra por el control de Internet adoptó la forma de censura de los contenidos "a lo bestia" con la excusa, afortunadamente cada vez menos creíble, de la pornografía infantil y del acceso a contenidos "inadecuados" por parte de menores de edad. Fue la malograda CDA (Ley de Decencia de las Comunicaciones), que el Tribunal Supremo norteamericano declaró sin ambages como inconstitucional, según destaca Carlos Sánchez Almeida en su artículo. En esa misma línea se situaban los programas censores a instalar en todos los ordenadores, pero, si no tienen un carácter coactivo, la gente pasará, como pasa de ellos. Se empieza ya a prescindir de muchos buscadores tradicionales.

La segunda guerra fue menos sutil, fue la guerra del dinero; la supervivencia en Internet parecía depender tan sólo de un "bisnesplan" de ensueño y de un talonario bien gordo. Fue la época de las puntocom y, tras dejarse un pastón que quieren recuperar, vieron que únicamente enseñando la billetera no bastaba para adueñarse de Internet.

La tercera guerra se sitúa en la línea de la segunda, pero buscando sus objetivos quizás de forma algo más sibilina. El objeto intermedio sigue siendo que sólo quienes tengan suficiente dinero puedan tener presencia activa en Internet y ello, ahora, se pretende obligando a todo el que quiera tener una Web a cumplir innumerables requisitos sometidos a la correspondiente multa en caso de incumplimiento.

Carlos Sánchez Almeida destaca en su artículo el ámbito de aplicación de la Ley, pero, aún más espeluznante que su texto articulado resulta la exposición de motivos: "Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información" [y tan amplio, como que abarca todo lo que esté en Internet, lo único que quedan fuera son las páginas con las fotos del gato y del bebé], que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información

por dicho medio (como el que efectúan los periódicos [iBrújula, por ejemplo] o revistas[Kriptopolis o makypress, por ejemplo] que pueden encontrarse en la Red), las actividades de intermediación relativas a la provisión de acceso a la Red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...). 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, los cuales normalmente no desempeñan una sola de estas actividades, sino varias, incluido el comercio electrónico."

En cristiano: ojo al dato, ay, ay ay, que los que pensáis que comercio electrónico haciendo no estáis, no os escapáis; hemos caído en la crisis puntocom, pero ahora os ha llegado vuestro turno.

De la versión anterior (18-01-01) el cambio más trascendente ha consistido en eliminar la referencia al carácter objetivo del concepto "servicios de la Sociedad de la Información", acaso porque sea incompatible con el espíritu de la norma de configurar una especie de Derecho especial en el marco de un sistema subjetivo de delimitación material, tal y como sucedió con el Derecho mercantil en sus orígenes. Tal situación podría encubrir una muestra de la intención inequícova de mercantilizar Internet.

En cualquier caso, para sus previsiones, la Ley pone de excusa (antes eran los menores que buscaban en Internet lo que enseñaban los quioskos y videoclubs) a los consumidores. Así, la Exposición de motivos dice que de la ley "destaca, por otra parte, su afán por proteger los intereses de los destinatarios de servicios, de forma que éstos puedan gozar de garantías suficientes a la hora de contratar un servicio o bien por Internet". Contratar un servicio, de acuerdo con el texto de la Ley, es leer este artículo.

Una oscura homogeneización que nos acecha. Nunca, antes que ahora, tenemos tanto en común quienes presentamos grandes diferencias; aprovechemos la oportunidad que nos dan para unirnos, porque puede que no haya otra.

La tercera guerra también la perderán. Esa Ley debe desvanecerse antes de que empiece su tramitación parlamentaria. El acceso a las Cortes de semejante engendro sería ya de por sí una burla al sistema democrático.

http://www.lssice.com/textos/analisis.html

conclusiones al análisis legal crísticas de Maestre
siones

La normativa que pretende instaurarse mediante la Directiva de Comercio Electrónico y la Ley de Servicios de la Sociedad de la Información (LSSI) constituye el mayor ataque sufrido contra la Internet libre desde los tiempos de la CDA norteamericana y supone un grave riesgo para el desarrollo pleno de una Sociedad en Red, que permita una progresión social y cultural, basada en la diversidad y en los principios democráticos.

La Ley de Servicios de la Sociedad de la Información pretende hacer de la información, cualquiera que sea su manifestación, una mera mercancía y convierte automáticamente en mercader a todo el que opere, desde cualquier perspectiva o circunstancia, con ella, a la vez que convierte en una actividad regulada cualquier iniciativa desarrollada en Internet.

El texto del Anteproyecto presenta un desmesurado ámbito de aplicación que, por momentos, supera el definido en el texto articulado de la Directiva que pretende transponer. Estimamos, por lo demás, que la Directiva debe incorporarse al ordenamiento Español, no mediante una única Ley de aplicación general a toda la actividad que se desarrolla en Internet, sino modificando la normativa relativa a cada institución que se vea afectada por la Directiva, a fin de adaptarse a las peculiaridades que reclama un nuevo medio como Internet.

La aplicación de la LSSI implicaría un grave retroceso en el desarrollo de Internet en España, condenando al cierre a numerosas iniciativas sin suficientes recursos financieros para atender con plenas garantías los requerimientos técnicos, administrativos y obligacionales que impone la Ley, a través de un desmesurado régimen sancionador. Los principales perjudicados por este texto son los pequeños y medianos empresarios y las iniciativas no comerciales, muchos de los cuales, de aprobarse la LSSI, se verían obligados al cierre, minando así las posibilidades de creación de un tejido empresarial propio adecuado a nuestras características.

La LSSI atribuye a la Administración excesivas facultades de restricción e intervención en la prestación de servicios, atribuyéndole, incluso, la potestad de cerrar un sitio web sin intervención judicial. Esta circunstancia implica una restricción inadmisible de la Libertad de Expresión y una sustracción de las competencias que actualmente tiene asumidas el poder judicial sobre las acciones limitativas de este Derecho Fundamental, consagrado en el artículo 20 de la Constitución. Esta circunstancia, sin perjuicio de otras, podría hacer que el texto actual fuera declarado inconstitucional.

Tal y como está redactada actualmente la Ley, en todo caso, incide enormemente en la configuración del marco legal para el ejercicio de los derechos reconocidos en el artículo 20 de la Constitución y, consecuentemente, su tramitación como Ley Ordinaria podría vulnerar la Reserva de Ley Orgánica contenida en el artículo 81 de la Constitución.

3. Los 12 países 'enemigos de Internet'

http://www.observatoriofucatel.cl/los-12-paises-enemigos-de-internet/

10/Marzo/2009 · Imprimir este artículo

EFE / París / La organización Reporteros sin Fronteras (RSF) publicó una lista de los que denomina "doce enemigos de Internet" por el control y la censura que ejercen sobre la red y el acceso a ella desde sus respectivos territorios. Se trata de Arabia Saudí, Birmania, China, Corea del Norte, Cuba, Egipto, Irán, Uzbekistán, Siria, Túnez, Turkmenistán y Vietnam, quienes, según la organización, "han transformado sus redes en Intranet, impidiendo que los internautas accedan a informaciones que se consideran 'indeseables'."Todos esos países ponen de manifiesto no solo su capacidad para

censurar la información, sino también la represión prácticamente sistemática de los internautas molestos", declara la organización en su informe.

En el caso cubano, RSF afirma que, aunque los ciudadanos de la isla pueden utilizar conexiones a Internet en hoteles turísticos y consultar páginas extranjeras, "la red se encuentra estrechamente vigilada por la Agencia Cubana de Supervisión y Control".

Este órgano, dependiente del Ministerio de Información, recuerda la organización, "decide la concesión de licencias, los precios y las posibilidades de conexión" y en la isla "hay un único proveedor de acceso a internet, ETEC SA, que alimenta una de las redes más restringidas del mundo".

Arabia Saudía, China

En cuanto a Arabia Saudí, RSF indica que las autoridades no han hecho oficial la práctica del filtrado de sitios "pero han optado por reprimir a los bloggers que se manifiestan en contra de su moral, sea cual sea la reivindicación".

El Gobierno chino "ostenta el liderazgo de la represión en Internet".Esta política, advierte RSF, "resulta muy disuasoria en un país que carece de código penal y detiene a los autores de 'contenidos que ofenden o violan' los principios de la religión islámica y las normas sociales".

El Gobierno chino "ostenta el liderazgo de la represión en Internet" y la organización advierte que "con la mayor población de internautas del mundo, el juego de la censura es uno de los más indecentes del mundo".

Los Juegos Olímpicos de Pekín en 2008 "permitieron, bajo presión de los medios de comunicación, el desbloqueo de algunos sitios de Internet para que los periodistas pudieran acceder a la información mundial" pero RSF constató que "fueron las versiones inglesas de Wikipedia, YouTube y Blogspot las que se hicieron accesibles".

"Las versiones chinas de esos sitios permanecieron bloqueadas, y la mayoría de los sitios informativos extranjeros en chino continúan inaccesibles", añade RSF, que afirma que "el sistema de la censura está muy organizado" en China.

Egipto, Irán, ¿Australia?

En Egipto, el "dinamismo" de la "blogosfera" de ese país en el panorama internacional "está muy lejos de ser una ventaja para sus bloggers, que se encuentran entre los más acosados del mundo", estima la organización.

En Australia se quiere obligar a los ISP a filtrar la conexión a Internet.Irán está a la cabeza de la represión en Internet en Oriente Medio, según la consideración que hace el informe de RSF, en cuyo informe se recuerda, que "según el consejero del fiscal general de Teherán, las autoridades bloquearon en 2008 cinco millones de sitios".

El informe dedica un apartado a la situación en Australia, donde recuerda que desde 2006 está en discusión un proyecto de ley "que obligará a todos los proveedores de acceso a filtrar la conexión a Internet en cada residencia" para "descartar cualquier contenido 'inapropiado".

El proyecto se justifica en nombre de "la lucha contra pederastia, la pornografía y la difamación, y en defensa de los derechos de autor", señala RSF, que dice se ha puesto en marcha "en un contexto en que la legislación sobre terrorismo ya permite graves atentados a la confidencialidad de la correspondencia privada".

Medidas 'preocupantes

Otros gobiernos -10 en total incluido el de Australia, que RSF afirma que están "bajo vigilancia"- también han adoptado medidas "preocupantes", porque, estima la organización, "pueden abrir la vía para que se cometan abusos".

"No es solo que la Red está cada vez más controlada, sino que también están apareciendo nuevas formas de censura, basadas en la manipulación de la información", agrega el informe de RSF.

Se trata de comentarios "teledirigidos" colgados en páginas muy consultadas y "pirateo informático orquestado por gobiernos censores", acciones que "están interfiriendo la información por internet", ha añadido la organización de defensa de la libertad de expresión.

RSF recuerda finalmente que actualmente hay 69 "ciberdisidentes" encarcelados por publicar información en internet y destaca el caso de China, que "conserva el triste récord de ser 'la mayor cárcel del mundo' para los 'ciberdisidentes', seguida de Vietnam e Irán".

4. El problema de la responsabilidad por los contenidos ilícitos en la web 2.0 y algunas propuestas de solución, por Lorenzo Cotino Hueso, 2009

Resumen. Es un problema determinar quién es responsable por los contenidos que los terceros integran en los distintos servicios de la web 2.0. La normativa y jurisprudencia actual no dan respuestas claras. Se trata de una cuestión clave para el futuro tanto de los servicios más empleados (*Google, Youtube, Facebook, Wikipedia*, etc.) cuanto el desarrollo de la web 2.0 misma. En el estudio se fijan los elementos clave según la normativa actual. También, se analiza la aplicabilidad en la red de vías jurisprudenciales clásicas de exención de responsabilidad por contenidos ilícitos: doctrina de "cartas al director", "reportaje neutral", así como la actitud diligente del prestador de servicios que alberga los contenidos integrados por terceros. Finalmente, se proponen criterios para el futuro, sobre la base de la preeminencia de la libertad de expresión. Se afirma que en general no hay que responsabilizar a los mediadores, que hay que proteger el anonimato en la red. Asimismo, se determinan criterios concretos para tener en cuenta en cada supuesto, bajo la idea de que hay que adaptarse a la naturaleza y circunstancias de cada caso en la red.

1. Introducción al problema y su importancia

1.1. El problema

La atribución de la responsabilidad por la difusión de contenidos ilícitos en la red[14] es una cuestión clave para la red misma. Es más, el problema cabe centrarlo en la

[14] Sobre responsabilidad, destaca Cavanillas 2005 y 2007. Centrado en EEUU, Peguera (2007).

responsabilidad que adquieren los variados prestadores de servicios que facilitan el acceso a los mismos, por los contenidos (textos, audios, vídeos, fotos, programas, etc.) integrados por terceros usuarios del servicio. De esta cuestión se hace depender el modelo de negocio de los servicios más empleados en la red (*Google, Youtube, Facebook, Wikipedia*, etc.) cuanto el desarrollo de la web 2.0 misma[15]. Hoy día internet se "*teje*" por no menos de un tercio de los internautas, "*heavy users*"[16], que participan generando y difundiendo contenidos[17]. Frente a la web 1.0, ahora se permite la integración, interacción y selección de contenidos por el usuario, que deja de ser un receptor, un consumidor de información, sino un "prosumidor" ("*prosumer*") de información, esto es, un híbrido de consumidor y productor de contenidos[18], en deliberación continua. "Sólo" hablamos de unos de diez millones de generadores de contenidos en España[19].

Integrando contenidos ilícitos se pone en riesgo jurídico a quien permite dicha participación. Alonso[20] recientemente ha bautizado una forma específica de acoso, "acoso informacional" o "*infomobbing*", al exigir responsabilidad a los alojadores de contenidos integrados por terceros y las vías de exigir la retirada de los mismos. Si se carga al responsable del sitio participativo de la responsabilidad de vigilar la licitud de los contenidos integrados por terceros, el efecto puede ser claro: sólo unos pocos, y muy difícilmente, tienen la capacidad personal y económica de llevar a cabo dicho control y filtro de los posibles ilícitos. Y lo que es peor, se produce un claro chilling effect, la tendencia autocensora sería lo natural: ante la duda, evitar posibles problemas. De este modo, muchos discursos quizá nocivos, pero lícitos[21], quedarían fuera.

1.2. Las dificultades materiales y jurídicas para la atribución y persecución de la responsabilidad

En internet se generan problemas casi insuperables de atribución y persecución de la responsabilidad civil, administrativa o penal, según se trate. Las dificultades materiales son muchas:

- los problemas para para perseguir contenidos ilícitos para el Derecho nacional, por estar ubicados fuera del ámbito territorial.

---

15 About web 2.0, Fumero (2007), Cerezo (2007).

16 Sobre *heavy users* Previte (2001), recientemente Ferran-Ferrer and Pérez-Montoro (2009).

17 Ver informes anuales, Fundación Telefónica (2008, p. 159). Un 29% de los internautas son "heavy users".

18 Bowman and Wills (2005, p 9).

19 Según los más recientes, en España, los conectados a internet son el 63,3% (38.7% en 2006), unos 28 millones de personas, un tercio viene a ser unos 10 millones. Febrero de 2009, http://www.internetworldstats.com/stats.htm)

20 Alonso (2008, p. 42).

21 Sobre la distinción lícito-nocivo, por todos, *Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones sobre contenidos ilícitos y nocivos en Internet*, de 16 de octubre de 1996 COM (96) 0487.

- Normalmente, quien integra el contenido lo hace de forma anónima . Conocer su número IP –si es que se puede- puede no ser suficiente para conocer la identidad.

- La autoría y difusión colaborativa de los contenidos de la web 2.0 conlleva que sea casi imposible de determinar el responsible del contenido y de su difusión.

A las anteriores barreras materiales y jurídicas, se une la grave insuficiencia normativa para la Unión Europea, a partir de la Directiva 2000/31/CE sobre el comercio electrónico.. Simplificando en lo posible, el esquema general es que el prestador de servicios de internet no tiene un deber de vigilar los contenidos que transmite (art. 15 Directiva comercio electrónico) ni es responsable de los mismos si son ilícitos, pero sí tiene el deber de retirar o bloquear los contenidos cuando las autoridades le comunican la ilicitud. Para aplicar este esquema, se parte de la premisa de que el "prestador de servicio de intermediación" (PSI)[22] no elabora o selecciona materialmente los contenidos discutibles[23], ni tiene conocimiento efectivo de la ilicitud del contenido. Sin embargo, la regulación no da respuesta a los problemas que hoy son los más habituales.

1.3. Las claves del problema jurídico de la responsabilidad de los contenidos

De una parte, el problema principal reside en determinar si cualquier sitio en la red que permite integrar contenidos de terceros usuarios (desde un foro clásico a *Youtube*) puede beneficiarse de las excenciones legales de resonsabilidad. Para ello, cabe determinar si este tipo de servicios son un "prestador de servicio de intermediación"[24] (art. 16 LSSICE), por "albergar datos proporcionados por el destinatario de este servicio"[25]. También pueden gozar de la exención general por

---

22 La terminología habitual es la de ISP, Internet Service Provider, pero lo cierto es que no coincide exactamente con el concepto se "prestador de servicios de intermediación" que es el empleado por la LSSICE, como a continuación se comenta.

23 En esta línea, el artículo 14 de la LSSICE exime de responsabilidad a los operadores de redes y proveedores de acceso "salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos", esto es, no se les exime en cuanto superen la neutralidad tecnológica de su función intermediadora[23]. Asimismo, por cuanto a los prestadores de servicios de alojamiento o almacenamiento de datos (art. 16) se señala que "2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador."

24 Según el anexo de definiciones de la LSSICE: b) "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.

25 Artículo 16. Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos: "1. Los prestadores de un servicio de intermediación consistente en

aplicación del artículo 17 LSSICE los servicios que "faciliten enlaces a otros contenidos o incluyan en los suyos directorios"[26]. Si el foro, blog, wiki, alojador de vídeos, imágenes, comentarios, etc. se beneficia del sistema de exención de responsabilidad de la LSSICE y no tendrá que vigilar los contenidos que alberga ni retirarlos hasta que tenga "conocimiento efectivo". De lo contrario, si estos servicios tan típicos de la red que permiten albergar contenidos no se consideran en el ámbito de estas excepciones, se les puede exigir una diligencia, control y responsabilidad por los mismos.

Considero en general que estos preceptos sí son aplicables a los servicios típicos en la web social y, por tanto, son beneficiarios de las exenciones de responsabilidad que la Directiva y la LSSICE establecen. Como consecuencia de la exención, no corresponde aplicar el regimen de responsabilidad que en su caso puediera correponder según el tipo de contenidos. En esta línea y de forma bastante certera son las sentencias que resuelven el caso "*mindoniense*" en 2008 y 2009[27].

De otra parte, para poder aplicar las exenciones de responsabilidad se precisa cierta neutralidad del sitio que alberga los contenidos, sin que los haya seleccionado o generado o no tenga un posible control de los mismos. No obstante, por definición las herramientas de la web 2.0 están diseñadas para permitir integrar contenidos por terceros, y sus usuarios lo incentivan (comentarios a noticias, a blogs, wikis, aportación de fotos, vídeos, etc.). Asimismo, lo habitual es la selección –automatizada o no- de contenidos de otros –como enlaces o contenidos sindicados a través de agregadores merced a *rss* y el lenguaje *xml*[28], etc.-. Así, no se da una completa neutralidad técnica, pero tampoco una colaboración deliberada para cometer ilícitos. Y en este terreno

---

albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: […]"

26 Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda: "1. 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 serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: […]"

27 Sobre afirmaciones insultantes contra el Alcalde de Mondoñedo (Lugo)en www.mindoniense.com. Sentencia de instancia del Juzgado de 1ª Instancia e Instrucción nº 1 de Mondoñedo y la apelación que confirma a la anterior por Sentencia de la Audiencia Provincial de Lugo, Sección 1ª, sentencia nº 538/2009. Todas las sentencias citadas, disponibles en www.documentostics.com

28 Como se señala en *Wikipedia* (voz "agregador", sin equivalente igual en inglés): "un agregador o agregador de noticias es un tipo de software para suscribirse a fuentes de noticias en formatos RSS, Atom y otros derivados de XML/RDF. El agregador reúne las noticias o historias publicadas en los sitios con redifusión web elegidos, y muestra las novedades o modificaciones que se han producido en esas fuentes web; es decir, avisa de qué webs han incorporado contenido nuevo desde nuestra última lectura y cuál es ese contenido. Esta información es la que se conoce como fuente web.

Un agregador es muy similar en sus presentaciones a los anteriores lectores de noticias (client newsreaders/NNTP), pero la tecnología XML y el web semántico los ha hecho más populares. Hoy en día, una enorme cantidad de blogs y sitios web ofrecen sus actualizaciones, que pueden ser fácilmente reunidas y administradas en un solo punto, como es el caso del servicio My Yahoo!, Google Reader, Netvibes y otros agregadores de escritorio que se listan más abajo."

intermedio y su incertidumbre jurídica ha quedado atrapada la web 2.0, a expensas de una actualización normativa de la Unión Europea, que ni se planea. Y la jurisprudencia española y europea[29] más que aclarar estos problemas, los evita o, como se verá, las decisiones judiciales son contradictorias. Por el contrario, en EEUU, el país de la libre expresión, ni la normativa, ni la jurisprudencia[30] rehúyen de estas cuestiones[31]. De un lado, hay sistemas bastante ágiles para barrer ilegalidades manifiestas de la red sin lesión de la libertad de expresión[32]. De otro lado, y también en favor de la libertad de expresión, la tendencia judicial es la de no responsabilizar por la integración de contenidos por terceros, a pesar de las consecuencias que ello genera y a la espera de mejores soluciones normativas[33].

2. Algunas vías para la exención de responsabilidad por los contenidos ilícitos difundidos

2.1. La aplicación de la doctrina constitucional de las cartas al director podría ilegalizar toda la web social

En el espacio destinado a las tradicionales "cartas al director", los periódicos no son responsables de lo publicado siempre que hayan sido diligentes en la identificación de quien remite la carta. De lo contrario, "al autorizar la publicación del escrito pese a no conocer la identidad de su autor ha de entenderse que el medio, por ese hecho, ha asumido su contenido."[34]. Esta jurisprudencia persigue, entre otros fines, que no se abra "la puerta a la creación de espacios inmunes"[35].

---

29 Al respecto, Cotino (2007).

30 Sólo hasta el año 2000 ya se sentaron las bases jurisprudenciales en más de una quincena de decisiones relativas a la libertad de expresión. Puede seguirse en general acudir a www.internetcases.com y www.internetlibrary.com, con extractos y referencias de las decisiones más importantes.

31 See, Balkin (2004), Sunstein (2001, 2003) and *Non authored* (2004).

32 Ver Sección 512 del *Copyright Act*, tras las modificaciones introducidas por la "*Digital Millennium Copyright Act"* en 1998.

33 Por todas, Stephen J. Barrett, et al. v. Ilena Rosenthal, S122953, 40 Cal.4th 33 (Cal. Sup. Ct., November 20, 2006), avaible at: http://www.internetlibrary.com/cases/lib_case447.cfm.
La sentencia que exime de responsabilidad al usuario individual que distribuye publicaciones en la red:
"We conclude that section 230 prohibits 'distributor' liability for Internet publications. We further hold that section 230(c)(1) immunizes individual 'users' of interactive computer services, and that no practical or principled distinction can be drawn between active and passive use. Accordingly, we reverse the Court of Appeal's judgment.
We acknowledge that recognizing broad immunity for defamatory republications on the Internet has some troubling consequences. Until Congress chooses to revise the settled law in this area, however, plaintiffs who contend they were defamed in an Internet posting may only seek recovery from the original source of the statement."

34 Sentencia del Tribunal Constitucional (STC) 3/1997, de 13 de enero FJ 3º.

35 STC 336/1993, fundamento jurídico 7.º,b.

La aplicación rigurosa de esta doctrina podría acabar con la *web* 2.0, puesto que es prácticamente imposible identificar a los usuarios que participan en la web 2.0, al tiempo de bastante negativo para el libre flujo de información y opinión.

La sentencia del caso "Mafius"[36] aplica con claridad la doctrina de las cartas al director para condenar penalmente al responsable del blog por permitir que las afirmaciones se hagan de forma anónima, especialmente por haberse configurado el foro de modo que no se recogía el número IP[37].

2.2. La aplicación de la jurisprudencia del "reportaje neutral" a quien remite o reproduce "neutralmente" a contenidos de terceros

La jurisprudencia del "reportaje neutral"[38] exime de responsabilidad al medio de comunicación que, con neutralidad, transmite referencias y afirmaciones procedentes de terceros. En abstracto, esta técnica podría hacerse valer cuando el sitio integre contenidos de otros, los enlace, utilice agregadores o los cada vez más generalizados, "*embed*"[39].

Nuestra experiencia judicial al respecto es escasa. Se rechazó de plano esta exención en el caso "*putasgae*", considerando que dotarse de contenidos externos implica hacerlos propios ("se procede a la recopilación para hacer propios los contenidos")[40]. El TS lo confirmó en diciembre de 2009, con una sentencia bastante mejorable[41]. Justo lo contrario que en el caso , *CCOO vs. El Corte Inglés*[42]. Se

---

36 Alumno de Instituto que crea foro en el que se insertan amenazas e injurias a un profesor. La sentencia de 30 de junio de 2006 del Juez de Primera Instancia e Instrucción de Arganda del Rey (Madrid) le condena por amenazas e injurias (en apelación sólo por injurias por la Audiencia) y considera editor al responsable del blog que no retuvo el número IP. Esta sentencia fue parcialmente revocada por la Audiencia provincial, si bien mantiene la responsabilidad del alumno, pero sólo por injurias.

37 La sentencia señala como factor para la atribución de la responsabilidad "que el propio editor en el Acto manifestó que había programado el blog para que se omita el apartado donde se recoge la dirección de IP lo que ha puesto de manifiesto en el citado blog reiteradamente como salvaguarda de impunidad."

38 Reportaje neutral, como dice el Alto Tribunal "es aquel en el que el medio de comunicación social «no hace sino reproducir lo que un tercer ha dicho o escrito» (STC 134/1999, FJ 4) o, en otros términos, cuando se limita a «la función de mero transmisor del mensaje» (STC 41/1994, de 15 de febrero, FJ 4)". Para medir la proximidad al reportaje neutral, se tiene en cuenta "el distanciamiento del articulista respecto de las opiniones" de las fuentes que utiliza (STC sentencia 76/2002, FJ 4º).

39 Difícilmente traducibles al español, *embed* significa "enclavar", "empotrar", "incrustar". Cada vez es más sencillo hacer *emebededs* de integración de otros contenidos.

40 Sentencia Audiencia Provincial Madrid núm. 50/2006 (Sección 19ª), de 6 febrero.

41 Ver "Otra sentencia contra la libertad de expresión, del TS, caso PUTASGAE"

http://www.cotino.net/2009/12/otra-sentencia-contra-la-libertad-de-expresion-del-ts-caso-putasgae/

En sentido diferente, el Tribunal Supremo en 2010, ver "Responsabilidad en internet y Chimo Bayo":

consideró como "simples mensajeros" de un contenido panfletario que ya estaba en la red a quienes lo reprodujeron en su web propia. Al respecto, es destacable el Caso canadiense Wayne Crookes,[43], sobre responsabilidad por enlaces a contenidos difamatorios. El juzgador señala que quien enlaza no está republicando o reeditando los contenidos enlazados, sino que más bien es como una nota a pie, siempre a salvo que la integración suponga una clara asunción y posicionamiento del contenido de lo enlazado[44].

El Tribunal Supremo, sentencia N°: 316/2010, de dieciocho de Mayo de 2010 , en el recurso de casacion Num:: 1873/2007, Ponente José Ramón Ferrándiz Gabriel, en el Caso Quejasonline.com, no hace responsible al foro de quejas bajo el argumento de que "Pues bien, la Audiencia Provincial no ha tenido en cuenta ese conjunto normativo [que incluye la contraria sentencia PUTASGAE] al declarar la responsabilidad de la demandada Ruboskizo, SL. Y, por ello, no ha extraído consecuencia alguna de que dicha sociedad no conociera ni pudiera razonablemente conocer, directamente o a partir de datos aptos para posibilitar la aprehensión de la realidad, que quien le suministraba el contenido lesivo para el demandante no era él, sino otra persona que utilizaba indebidamente su nombre con el ánimo de perjudicarle; ni de que, conocedora con posterioridad de esa realidad, merced al requerimiento del perjudicado, retirase el comentario sin tacha de negligencia."

A mi juicio, la exención del reportaje neutral no hay que reservarla a los "medios de comunicación" clásicos y cabe extenderla para los diversos usos de la web social.

---

http://www.cotino.net/2010/05/responsabilidad-en-internet-y-chimo-bayo/

42 Sentencia Tribunal Superior de Justicia Madrid núm. 663/2003 (Sala de lo Social), de 23 julio.

43 Wayne Crookes and West Coast Title Search Ltd. Vs. Wikimedia Foundation Inc. And Anonymous, Supreme Court Of British Columbia, 2008 BCSC 1424 Date: 2008. Avaible at: documentostics.com/component/option,com.../task.../gid,1455/

44 Así, se afirma:

[29] A hyperlink is like a footnote or a reference to a website in printed material such as a newsletter. The purpose of a hyperlink is to direct the reader to additional material from a different source. The only difference is the ease with which a hyperlink allows the reader, with a simple click of the mouse, to instantly access the additional material.

[30] Although a hyperlink provides immediate access to material published on another website, this does not amount to republication of the content on the originating site. This is especially so as a reader may or may not follow the hyperlinks provided.

[31] I conclude that the reasoning of the Court of Appeal in Carter leads to the same conclusion on the narrower issue before me. Readers of a newsletter, whether in paper form or online, who read of a reference to a third party website, may go to that website. I conclude that that does not make the publisher of the web address a publisher of what readers find when they get there.

[33] As the Court of Appeal observed in Carter, citing the proposition of the New York cases MacFadden v. Anthony and Kline v. Biben, "reference to an article containing defamatory content without repetition of the comment itself should not be found to be a republication of such defamatory content".

[34] I do not wish to be misunderstood. It is not my decision that hyperlinking can never make a person liable for the contents of the remote site. For example, if Mr. Newton had written "the truth about Wayne Crookes is found here" and "here" is hyperlinked to the specific defamatory words, this might lead to a different conclusion.

Ello, sin perjuicio, claro está, de que de sea necesario contextualizar cada supuesto y no se dé mala fé y abuso de derecho a través de esta vía (art. 7 Código Civil)[45].

2.3. La diligencia del ISP o alojador como criterio de responsabilización

En ocasiones, los jueces varían la responsabilidad en razón de la actitud de quien alberga la información conflictiva. A veces, se valora positivamente la plena colaboración para cumplir lo que los jueces soliciten respecto de los contenidos. Así, en el caso *Weblisten*[46]. Por el contrario, en el caso "*putasgae"*, el tribunal no tiene en cuenta que la Asociación de internautas retiró los contenidos nada más conocer que había una demanda. En en el caso "*aprendizmason.org"*[47], se tuvo en cuenta la voluntaria actitud del ISP, que comunicó al autor de contenidos que el afectado había solicitado su retirada por su ilicitud.

En el caso "alasbarricadas.org vs. Ramoncín" (conocido artista exdirectivo y favorable a la SGAE)[48] se hizo responsible del contenido de un foro a la web por una "falta de diligencia" muy común en la red:

- no actualizar información que se aporta en el registro de su dominio,
- no probar que el mail de contacto que figuraba en la web fuera un medio de contacto eficaz,
- no "contar con un moderador u otros filtros
- o que los contenidos se actualicen a diario o semanalmente, o las características de su sistema o aplicación informática de modo que se evite prolongar en el tiempo contenidos ilícitos".

Lo más preocupante es la falta de sustento legal de estas exigencias y que se argumenta forzadamente que la exención de responsabilidad de la Directiva y la LSSICE se vincula a la información obligatoria (art. 5 Directiva; art. 10 LSSICE)[49].

---

45 Artículo 7: "1. Los derechos deberán ejercitarse conforme a las exigencias de la buena fe.
2. La ley no ampara el abuso del derecho o el ejercicio antisocial del mismo. Todo acto u omisión que por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho, con daño para tercero, dará lugar a la correspondiente indemnización y a la adopción de las medidas judiciales o administrativas que impidan la persistencia en el abuso."

46 Auto Juzgado de lo Mercantil nº 2 de Madrid, de 3 noviembre 2004.

47 Sentencia Audiencia Provincial Madrid núm. 835/2005 (Sección 14ª), de 20 diciembre, caso *aprendizmason*.org.

48 Sentencia del Juzgado de Primera Instancia nº 44 de Madrid, de 13 de septiembre.

En sentido contrario, la sentencia de instancia del caso "Mindoniense" contradice expresamente estos deberes de diligencia[50]. En este caso, aunque sin relevancia, se subraya la buena fe de la página demandada porque contaba con la herramienta informática de censura previa denominada "Word Censors".

Considero que se dan los presupuestos de la exención de responsabilidad prevista por la LSSICE y la Directiva, no procede un análisis de la concurrencia de responsabilidad por el parámetro de diligencia que pueda corresponder (diligencia ex artículo 1902 CC[51], responsabilidad en cascada de la Ley de prensa[52], etc.). Esta solución no impide, evitar el abuso de derecho y la mala fe para eximirse de responsabilidades.

3. Algunas propuestas de futuro

Pese a la inercia sociológica y jurídica de reservar las libertades de expresión e información para los medios de comunicación, el punto de partida jurídico debe ser que estas libertades se proyectan a los usos y servicios en internet[53]. La función social o constitucional que desarrollan los medios de comunicación en la sociedad democrática ha justificado para los tribunales su protección más intensa por estas libertades. Hoy día esta función se desarrolla en internet y no sólo los medios institucionalizados. También, y como punto de partida jurídico, la libertad de expresión también protege el anonimato en la red, como Roig Batalla ha sostenido sobre la jurisprudencia de EEUU (Roig, 2007). Pese a que el anonimato se aproveche para cometer ilícitos, también ha servido

---

49 "El art. 16 debe ponerse en relación con el art. 10 de la referida Ley en cuanto al deber de información general que impone al prestador de servicios de la sociedad de la información, relativo a sus datos de identidad o localización, con el fin de garantizar la posibilidad de cumplir de modo diligente con la obligación de eliminar todo contenido ilícito o atentatorio al honor de determinada persona y eludir su misma responsabilidad, evitando su contribución en su difusión o en que ésta se prolongue en el tiempo. Dicho deber es el que posibilita que el mismo prestador pueda tener conocimiento directo e inmediato de la lesión por parte del afectado, pudiendo así en virtud de la misma comunicación del afectado cesar de modo inmediato en su actuación.Actuación del titular de la web que le ha impedido cumplir diligentemente con su deber de retirada del material difamatorio".

50 "debiendo quedar al margen la cuestión relativa a la existencia o no del incumplimiento por los demandados de las obligaciones prevenidas en el artículo 10 de la LSSI, (ya que, en su caso, debería dar lugar a la correspondiente responsabilidad administrativa, siendo esta una cuestión distinta a la petición de exacción de responsabilidad civil efectuada por la representación de la actora".

51 Artículo 1902: "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia está obligado a reparar el daño causado."

52 Artículo 65.2 de la Ley de 18 marzo 1966, del Ordenamiento Jurídico de la Prensa e Imprenta: "De la responsabilidad civil en materia de Prensa e Imprenta y de la patrimonial del Estado":
"2.- La responsabilidad civil por actos u omisiones ilícitos, no punibles, será exigible a los autores, directores, editores, impresores, e importadores o distribuidores de impresos extranjeros, con carácter solidario."

53 En esta dirección, con acierto, la reciente sentencia del TJCE (Gran Sala) de 16 de diciembre de 2008, cuestión prejudicial asunto C 73/07, nº 58-60.

para forjar una red como sinónimo de libertad y participación[54]. "El anonimato es el escudo frente a la tiranía de la mayoría", por lo que sus restricciones deben someterse a un escrutinio estricto [55]. Esta jurisprudencia ya se ha proyectado para un foro en internet[56].

Ya sobre tales bases, en el ámbito de la responsabilidad en la red, la Directiva de comercio electrónico y la LSSICE son insuficientes pero no se prevé tal reforma. A mi juicio y en favor de la libertad de expresión[57], el criterio general debe ser el de no atribuir responsabilidad a quienes albergan contenidos de terceros. Siguiendo la estela de EEUU, parece mejor contar con mecanismos ágiles para barrer contenidos claramente ilícitos en la red. También, para el análisis de cada supuesto hay que adecuarse a cada uso y naturaleza y contenido de lo que hay en internet, fijar la atención en muchas circunstancias que pueden tener relevancia jurídica, entre otras muchas:

-la voluntariedad (directa o en la confección del sitio web),

-la estructura más o menos automatizada de una sindicación de contenidos, más o menos selectiva de los mismos,

-la diligencia en la selección de contenidos o en la confección técnica de la selección,

-la participación real el los mismos, la significancia de los contenidos conflictivos en el marco de la cantidad de los contenidos seleccionados,

-la participación real en la generación de contenidos los mismos, la significancia de los contenidos conflictivos en el marco de la cantidad de los contenidos seleccionados

-los indicios que llevan a pensar en el conocimiento efectivo material de los contenidos y su posibilidad de control,

-el hecho de que esos contenidos estén más o menos difundidos en otros sitios,

-el nivel de acceso y relevancia en la red de quien los difunde.

-el uso habitual de ese sitio web (no es lo mismo insultar en una cantina a las dos de la madrugada que en mitad de clase) y la posibilidad de respuesta del afectado en el medio que es la red.

-La misma posibilidad de réplica y argumentación por el afectado en la *web* social.

Algunos de estos elementos se pueden observar en la casuística judicial española y las circunstancias del medio sirven para analizar la responsabilidad. En el caso *foro*

---

54 Wolton, quoted by Fernández, J. J. (2004, p. 192). Sobre el tema, Barrat (2004), Morón (2002).

55 Sentencia del Tribunal Supremo de los EEUU McINTYRE v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

56 Caso John Doe nº1 v. Cahill WL 2455266 (Delaware, October 5, 2005). http://internetcases.com/library/cases/2005-10-05-cahill_v_doe.html, última. Doe (nombre anónimo) publicó textos en un blog donde criticaba a un concejal por su gestión. La Corte requirió un test estricto para levantar el velo de su anonimato para perseguirlo.

57 About freedom of speech and the internet in Spain Fernández-Esteban (1998 a, 1998 b, 1999), Corredoira (1998)Boix (2002), Boix and López, G. (2006), García-Morales (2006) and some of my books and studies.

para desahogo[58] no se condenó porque los insultos estaban "dentro de una página *web* destinada específicamente a servir como tribuna de quejas o descarga de iras contenidas entre usuarios que se registren. Dicho con simpleza, foro para manifestar los propios descontentos o simplemente hablar mal". En el caso *quejasonline.com* [59] se exime de responsabilidad al considerar que era un medio informativo. En otros casos, la difusión bastante masiva de información perjudicial para una persona a través del mail ha sido considerada fuera de la libertad de expresión[60].

En la sentencia del *caso de la carta colgada en internet del colegio de las Ursulinas contra una constructora*[61] se tiene en cuenta que "la persona que accede a la página de internet del denunciado- apelante lo hace por su propia voluntad y, por lo demás, se podría ver contrarrestado por la información dada por la otra parte." Así, en la línea americana del caso *John Doe nº 1 v. Cahill.* En el caso *Plataforma Regional Pro-Identidad Leonesa*[62], pese a que los argumentos sean mejorables, cuanto menos se contextualiza el modo de comunicación que implica internet[63]. A mi juicio se trata de nuevo de una línea proclive a la contextualización pro-libertate de la red frente a los medios de comunicación clásicos y a la necesidad de adecuarse y adaptarse a la naturaleza diversa de los usos de internet.

5. Alguna regulación general relevante para la libertad de expresión e información (aplicable a internet)

Protección civil (Ley orgánica 1/1982)

LEY ORGÁNICA 1/1982, DE 5 DE MAYO, DE PROTECCIÓN CIVIL DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN

Artículo séptimo

---

58 Auto de la Audiencia Provincial de Barcelona núm. 339/2005 (Sección 6ª), de 24 de mayo, razonamiento jurídico segundo.

59 Auto Audiencia Provincial Madrid núm. 36/2006 (Sección 2ª), de 31 enero. Textos en *quejasonline.com* sobre la actuación errónea de uan constructora.

60 Así, caso de ofensas en el ámbito profesores universitarios por medio de mensajes colectivos a través del correo electrónico, la Sentencia Audiencia Provincial Granada núm. 144/2006 (Sección 4), de 7 abril excluye que esté en juego la libre expresión.

61 Apelación resuelta por sentencia de la Audiencia Provincial Álava núm. 55/2006 (Sección 1ª), de 11 abril.

62 La sentencia de la Audiencia Provincial de León núm. 302/2005 (Sección 2ª), de 19 diciembre resuelve un recurso de apelación frente a sentencia de instancia que desestimaba una acción de rectificación. Se pretendía que se rectificasen unos juicios históricos que figuraban en la web de una fundación.

63 Ahí en concreto, se dice que la *web* de una plataforma política no va dirigida a un público numeroso y heterogéneo (lo cual es cierto y relevante), ni se le puede exigir veracidad (lo cual es discutible, si bien se debe modular el entendimiento de ésta para no interrumpir el proceso de libre expresión en internet).

Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

Uno. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

Tres. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

Cuatro. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

Cinco. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.

Seis. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

Siete. *Modificado por la Ley Orgánica 10/1995.* La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Artículo octavo

Uno. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante.

Dos. En particular, el derecho a la propia imagen no impedirá:

a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.

c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

Artículo noveno

Uno. La tutela judicial frente a las intromisiones ilegítimas en los derechos a que se refiere la presente ley podrá recabarse por las vías procesales ordinarias o por el procedimiento previsto en el artículo cincuenta y tres, dos, de la Constitución. También podrá acudirse, cuando proceda, al recurso de amparo ante el Tribunal Constitucional.

Dos. La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones

ulteriores. Entre dichas medidas podrán incluirse las cautelares encaminadas al cese inmediato de la intromisión ilegítima, así como el reconocimiento del derecho a replicar, la difusión de la sentencia y la condena a indemnizar los perjuicios causados.

Tres. La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta en su caso, la difusión o audiencia del medio a través del que se haya producido. También se valorará el beneficio que haya obtenido el causante de la lesión como consecuencia de la misma.

Cuatro. El importe de la indemnización por el daño moral, en el caso del artículo cuarto, corresponderá a las personas a que se refiere su apartado dos y, en su defecto, a sus causahabientes, en la proporción en que la sentencia estime que han sido afectados. En los casos del artículo sexto, la indemnización se entenderá comprendida en la herencia del perjudicado.

Cinco. Las acciones de protección frente a las intromisiones ilegítimas caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas.

Derecho de rectificación

LEY ORGÁNICA 2/1984, DE 26 DE MARZO, REGULADORA DEL DERECHO DE RECTIFICACIÓN

Articulo primero

Toda persona natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan , que considera inexactos y cuya cuya divulgación pueda causarle perjuicio .

Podrán ejercitar el derecho de rectificación el perjuicio aludido o su representante y, si hubiese fallecido aquel, sus herederos o los representantes de estos.

Artículo segundo.

El derecho se ejercitara mediante la remisión del escrito de rectificación al director del medio de comunicación dentro de los siete días naturales siguientes al de publicación o difusión de la información que se desea rectificar , de forma tal que permita tener constancias de su fecha y de su recepción.

La rectificación deberá limitarse a los hechos de la información que se desea rectificar.. Su extensión no excederá sustancialmente de la de ésta, salvo que sea absolutamente necesario.

Articulo tercero.

Siempre que el derecho se ejercite de conformidad con lo establecido en el articulo anterior, el director del medio de comunicación social deberá publicar o difundir íntegramente la rectificación, dentro de los tres días siguientes al de su recepción, con relevancia semejante a aquella en que se publico o difundió la información que se rectifica , sin comentarios ni apostillas.

Si la información que se rectifica se difundió en publicación cuya periodicidad no permita la divulgación de la rectificación en el plazo expresado, se publicara esta en el numero siguiente

Si la noticia o información que se rectifica se difundió en el espacio radiofonico o de televisión que no permita, por la reciprocidad de su emisión, divulgar la rectificación en el plazo de tres días, podrá exigir el rectificante que se difunda en espacio de audiencia y relevancia semejantes, dentro de dicho plazo .

La publicación o difusión de la rectificación será siempre gratuita.

Articulo cuarto.

Si, en los plazos señalados en el articulo anterior, no se hubiera publicado o divulgado la rectificación o se hubiese notificado expresamente por el director o responsable del medio de comunicación social que aquella no será difundida, o se haya publicado o divulgado sin respetar lo dispuesto en el articulo anterior, podrá el perjudicado ejercitar la acción de rectificación dentro de los siete días hábiles siguientes ante el Juez de Primera Instancia de su domicilio o ante el del lugar donde radique la dirección del medio de comunicación

Articulo quinto.

La acción se ejercitará mediante escrito, sin necesidad de Abogado ni Procurador, acompañando la rectificación y la justificación de que se remitió en el plazo señalado;; se presentara igualmente la información rectificada si se difundió por escrito; y, en otro caso, reproducción o descripción de la misma tan fiel como sea posible .

El Juez, de oficio y sin audiencia del demandado, dictará auto no admitiendo a tramite la demanda si se considera incompetente o estima la rectificación manifiestamente improcedente.. En otro caso convocara al rectificante, .al director del medio de comunicación o a sus representantes a juicio verbal, que se celebrara dentro de los siete días siguientes al de la petición. . La convocatoria se hará telegráficamente, sin perjuicio de la urgente remisión, por cualquier otro medio, de la copia de la demanda a la parte demandada .

Cuando el Juez de Primera Instancia hubiese declarado su incompetencia podrá el perjudicado acudir al órgano competente dentro de los siete días hábiles siguientes al de la fecha de notificación de la correspondiente resolución, en la cual se deberá expresar el órgano al que corresponda el conocimiento del asunto.

Articulo sexto.

El juicio se tramitará conforme a lo establecido en la Ley de Enjuiciamiento Civil para los juicios verbales, con las siguientes modificaciones:

a) El Juez podrá reclamar de oficio que el demandado remita o presente la información enjuiciada, su grabación o reproducción escrita.

b) Solo se admitirán las pruebas que, siendo pertinentes, puedan practicarse en el acto.

c) La sentencia se dictará en el mismo o al siguiente día del juicio.

El fallo se limitará a denegar la rectificación o a ordenar su publicación o difusión en la forma y plazos previstos en el articulo 3º de esta Ley, contados desde la notificación de la sentencia que impondrá el pago de las costas a la parte cuyos pedimentos hubiesen sido totalmente rechazados .

La sentencia estimatoria de la petición de rectificación deberá cumplirse en sus propios términos .

El objeto de este proceso es compatible con el ejercicio de las acciones penales o civiles de otra naturaleza que pudieran asistir al perjudicado por los hechos difundidos.

Articulo séptimo.

No será necesaria la reclamación gubernativa previa cuando la información que se desea rectificar se haya publicado o difundido en un medio de comunicación de titularidad publica.

Articulo octavo.

No serán susceptibles de recurso alguno las resoluciones que dicte el Juez en este proceso, salvo el auto al que se refiere el párrafo segundo del articulo 5º ., que será apelable en ambos efectos , y la sentencia, que lo será en un solo efecto, dentro de los tres y cinco días siguientes, respectivamente, al de su notificación, conforme a lo dispuesto en las secciones primera y tercera del Titulo sexto del libro II de la Ley de Enjuiciamiento Civil. . La apelación contra el auto a que se refiere el articulo 5º . se sustanciará sin audiencia del demandado.

Disposición Derogatoria.

Quedan derogados los artículos 58 a 62 de la Ley 14/1966, de 18 de marzo; el articulo 25 de la Ley 4/1980, de 10 de enero , sobre el Estatuto de la Radio y la Televisión ; los Decretos 745/1966, de 31 de marzo, y 746/1966, de la misma fecha, y el numero 1 del articulo 566 del Código Penal, así como cuantas disposiciones se opongan a lo establecido en esta Ley.

Palacio de la Zarzuela, Madrid, a 26 de Marzo de 1984.

- JUAN CARLOS R.-

EL Presidente del Gobierno , Felipe González Márquez

Código penal, calumnia, injuria

De la calumnia

Artículo 205.

Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 206.

Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de seis a veinticuatro meses, si se propagaran con publicidad, y, en otro caso, con multa de cuatro a diez meses.

Artículo 207.

El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado.

CAPÍTULO II

De la injuria

Artículo 208.

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 209.

Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses.

Artículo 210.

El acusado de injuria quedará exento de responsabilidad probando la verdad de las imputaciones cuando éstas se dirijan contra funcionarios públicos sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de faltas penales o de infracciones administrativas.

CAPÍTULO III

Disposiciones generales

Artículo 211.

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212.

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

...

Artículo 216.

En los delitos de calumnia o injuria se considera que la reparación del daño comprende también la publicación o divulgación de la sentencia condenatoria, a costa del condenado por tales delitos, en el tiempo y forma que el Juez o Tribunal consideren más adecuado a tal fin, oídas las dos partes.

Xenofobia, contenidos nocivos

Código Penal (arts. 22, 314, 510-512, 607)

Artículo 22.

Son circunstancias agravantes:

Cometer el delito por motivos racistas, antisemitas u otra clase de discriminación referente a la ideología, religión o creencias de la víctima, la etnia, raza o nación a la que pertenezca, su sexo u orientación sexual, o la enfermedad o minusvalía que padezca.

Artículo 314.

Los que produzcan una grave discriminación en el empleo, público o privado, contra alguna persona por razón de su ideología, religión o creencias, su pertenencia a una etnia, raza o nación, su sexo, orientación sexual, situación familiar, enfermedad o minusvalía, por ostentar la representación legal o sindical de los trabajadores, por el parentesco con otros trabajadores de la empresa o por el uso de alguna de las lenguas oficiales dentro del Estado español, y no restablezcan la situación de igualdad ante la Ley tras requerimiento o sanción administrativa, reparando los daños económicos que se hayan derivado, serán castigados con la pena de prisión de seis meses a dos años o multa de seis a doce meses.

Artículo 510.

1. Los que provocaren a la discriminación, al odio o a la violencia contra grupos o asociaciones, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia o raza, su origen nacional, su sexo, orientación sexual, enfermedad o minusvalía, serán castigados con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. Serán castigados con la misma pena los que, con conocimiento de su falsedad o temerario desprecio hacia la verdad, difundieren informaciones injuriosas sobre grupos o asociaciones en relación a su ideología, religión o creencias, la pertenencia de sus miembros a una etnia o raza, su origen nacional, su sexo, orientación sexual, enfermedad o minusvalía.

Artículo 511.

1. Incurrirá en la pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años el particular encargado de un servicio público que deniegue a una persona una prestación a la que tenga derecho por razón de su ideología, religión o creencias, su pertenencia a una etnia o raza, su origen nacional, su sexo, orientación sexual, situación familiar, enfermedad o minusvalía.

2. Las mismas penas serán aplicables cuando los hechos se cometan contra una asociación, fundación, sociedad o corporación o contra sus miembros por razón de su ideología, religión o creencias, la pertenencia de sus miembros o de alguno de ellos a una etnia o raza, su origen nacional, su sexo, orientación sexual, situación familiar, enfermedad o minusvalía.

3. Los funcionarios públicos que cometan alguno de los hechos previstos en este artículo, incurrirán en las mismas penas en su mitad superior y en la de inhabilitación especial para empleo o cargo público por tiempo de dos a cuatro años.

Artículo 512.

Los que en el ejercicio de sus actividades profesionales o empresariales denegaren a una persona una prestación a la que tenga derecho por razón de su ideología, religión o creencias, su pertenencia a una etnia, raza o nación, su sexo, orientación sexual, situación familiar, enfermedad o minusvalía, incurrirán en la pena de inhabilitación especial para el ejercicio de profesión, oficio, industria o comercio, por un período de uno a cuatro años.

Artículo 607.

1. Los que, con propósito de destruir total o parcialmente a un grupo nacional, étnico, racial o religioso, perpetraren alguno de los actos siguientes, serán castigados:

Con la pena de prisión de quince a veinte años, si mataran a alguno de sus miembros.

Si concurrieran en el hecho dos o más circunstancias agravantes, se impondrá la pena superior en grado.

Con la prisión de quince a veinte años, si agredieran sexualmente a alguno de sus miembros o produjeran alguna de las lesiones previstas en el artículo 149.

Con la prisión de ocho a quince años, si sometieran al grupo o a cualquiera de sus individuos a condiciones de existencia que pongan en peligro su vida o perturben gravemente su salud, o cuando les produjeran algunas de las lesiones previstas en el artículo 150.

Con la misma pena, si llevaran a cabo desplazamientos forzosos del grupo o sus miembros, adoptaran cualquier medida que tienda a impedir su género de vida o reproducción, o bien trasladaran por la fuerza individuos de un grupo a otro.

Con la de prisión de cuatro a ocho años, si produjeran cualquier otra lesión distinta de las señaladas en los números 2 y 3 de este apartado.

2. La difusión por cualquier medio de ideas o doctrinas que nieguen o justifiquen los delitos tipificados en el apartado anterior de este artículo, o pretendan la rehabilitación de regímenes o instituciones que amparen prácticas generadoras de los mismos, se castigará con la pena de prisión de uno a dos años.

LEY ORGÁNICA 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en españa y su integración social

Artículo 3. Derechos de los extranjeros e interpretación de las normas.

1. Redactado conforme a la Ley Orgánica 8/2000, de 22 de diciembre Los extranjeros gozarán en España de los derechos y libertades reconocidos en el Título I de la Constitución en los términos establecidos en los Tratados internacionales, en esta Ley y en las que regulen el ejercicio de cada uno de ellos. Como criterio interpretativo general, se entenderá que los extranjeros ejercitan los derechos que les reconoce esta Ley en condiciones de igualdad con los españoles.

2. Las normas relativas a los derechos fundamentales de los extranjeros se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y con los Tratados y Acuerdos internacionales sobre las mismas materias vigentes en España, sin que pueda alegarse la profesión de creencias religiosas o convicciones ideológicas o culturales de signo diverso para justificar la realización de actos o conductas contrarios a las mismas.

Artículo 23. Actos discriminatorios. Redactado conforme a la Ley Orgánica 8/2000, de 22 de diciembre

1. A los efectos de esta Ley, representa discriminación todo acto que, directa o indirectamente, conlleve una distinción, exclusión, restricción o preferencia contra un extranjero basada en la raza, el color, la ascendencia o el origen nacional o étnico, las convicciones y prácticas religiosas, y que tenga como fin o efecto destruir o limitar el reconocimiento o el ejercicio, en condiciones de igualdad, de los derechos humanos y de las libertades fundamentales en el campo político, económico, social o cultural.

2. En cualquier caso, constituyen actos de discriminación:

a) Los efectuados por la autoridad o funcionario público o personal encargados de un servicio público, que en el ejercicio de sus funciones, por acción u omisión, realice cualquier acto discriminatorio prohibido por la ley contra un ciudadano extranjero sólo por su condición de tal o por pertenecer a una determinada raza, religión, etnia o nacionalidad.

b) Todos los que impongan condiciones más gravosas que a los españoles, o que impliquen resistencia a facilitar a un extranjero bienes o servicios ofrecidos al público, sólo por su condición de tal o por pertenecer a una determinada raza, religión, etnia o nacionalidad.

c) Todos los que impongan ilegítimamente condiciones más gravosas que a los españoles o restrinjan o limiten el acceso al trabajo, a la vivienda, a la educación, a la formación profesional y a los servicios sociales y socioasistenciales, así como a cualquier otro derecho reconocido en la presente Ley Orgánica, al extranjero que se

encuentre regularmente en España, sólo por su condición de tal o por pertenecer a una determinada raza, religión, etnia o nacionalidad.

d) Todos los que impidan, a través de acciones u omisiones, el ejercicio de una actividad económica emprendida legítimamente por un extranjero residente legalmente en España, sólo por su condición de tal o por pertenecer a una determinada raza, religión, etnia o nacionalidad.

e) Constituye discriminación indirecta todo tratamiento derivado de la adopción de criterios que perjudiquen a los trabajadores por su condición de extranjeros o por pertenecer a una determinada raza, religión, etnia o nacionalidad.

6. Regulación específica de la responsabilidad y contenidos alojados en la red en la LSSICE

LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (extractos)

TITULO II

Prestación de servicios de la sociedad de la información

CAPITULO I

Principio de libre prestación de servicios

Artículo 6. No sujeción a autorización previa.

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a 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.

Artículo 7. Principio de libre prestación de servicios.

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo 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 en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

(LMISI 2007)

«Artículo 8. Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) 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

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

Nuevo 2. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

Anterior 2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de datos procedentes de un prestador establecido en otro Estado, el órgano competente estimara necesario impedir el acceso desde España a los mismos, podrá ordenar a los prestadores de servicios de intermediación establecidos en España, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que tomen las medidas necesarias para impedir dicho acceso.

Será de aplicación lo dispuesto en el artículo 11 cuando los datos que deban retirarse o el servicio que deba interrumpirse procedan de un prestador establecido en España.

3 Las medidas de restricción a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

3. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

Anterior

4. Fuera del ámbito de los procesos judiciales, cuando se establezcan restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, se seguirá el siguiente procedimiento

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

4. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

5. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.»

Artículo 8. Restricciones a la prestación de servicios.

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran Los principios a que alude este apartado son los siguientes

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

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

c) El respeto ala dignidad de la persona yal principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y

familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

4. Fuera del ámbito de los procesos judiciales, cuando se establezcan restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, se seguirá el siguiente procedimiento

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo en el plazo de quince días desde su adopción. Asimismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

«Artículo 11. Deber de colaboración de los prestadores de servicios de intermediación.

1. Cuando un órgano competente (ANTERIOR) *por razón de la materia* hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores (*ANTES , directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología)*, que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente. (*antes: que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran)*

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la

información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

Nuevo 2007 LMISI En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

(ANTES) En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.»

Antigua redacción previa a LMISI

Artículo 11. Deber de colaboración de los prestadores de servicios de intermediación.

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las funciones que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, podrá ordenar a dichos prestadores, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de

actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

Artículo 12. Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas. (derogado, regulación básica en Ley 25/2007)

Nuevo

«Artículo 12 bis. Obligaciones de información sobre seguridad.

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.»

SECCIÓN 2.º RÉGIMEN DE RESPONSABILIDAD

Artículo 13. Responsabilidad de los prestadores de los servicios de la sociedad de la información.

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. Responsabilidad de los operadores de redes y proveedores de acceso.

1. Los operadores de redes de telecomunicaciones 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 ésta no serán responsables por 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 entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.

2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen 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.

Artículo 15. Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.

Los prestadores de un servicio de intermediación 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 los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) No modifican la información.

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

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

d) No interfieren 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) Retiran la información que hayan almacenado o hacen 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.

Artículo 16. Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.

1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es llícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los

datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2 La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.

Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.

1. 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 serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Nuevo LMISI

«2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.»

Antiguo 2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

CAPITULO III

Códigos de conducta

Artículo 18. Códigos de conducta.

1. Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta 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.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.

Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.

Nuevo LMISI

«3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.»

(Anterior: 3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales en la Comunidad Europea, con objeto de darles mayor difusión.

TITULO VIl

Infracciones y sanciones

Artículo 37. Responsables.

Los prestadores de servicios de la sociedad de la información están sujetos al régimen sancionador establecido en este Título cuando la presente Ley les sea de aplicación.

Artículo 38. Infracciones.

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.

2. Son infracciones muy graves

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

b) El incumplimiento de 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.

c) 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, prevista en el artículo 12.

d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a) El incumplimiento de lo establecido en los párrafos a) y f) del artículo 10. 1.

b) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a destinatarios que no hayan autorizado o solicitado expresamente su remisión, o el envío, en el plazo de un año, de más de tres

comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando éste no hubiera solicitado o autorizado su remisión.

c) 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 el artículo 27.

d) 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.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

4. Son infracciones leves

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan solicitado o autorizado expresamente su remisión, cuando no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 2 7. 1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

Artículo 39. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el «Boletín Oficial del Estado», o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción en dos periódicos cuyo ámbito de difusión coincida c6n el de actuación de la citada Administración pública o en la página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, por el número de usuarios o de contratos afectados, y la gravedad del ilícito.

3. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que

hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

Artículo 40. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios

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) Volumen de facturación a que afecte la infracción cometida.

Artículo 4l. Medidas de carácter provisional.

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

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

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento,

que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 43. Competencia sancionadora.

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo.

Artículo 44. Concurrencia de infracciones y sanciones.

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. Prescripción.

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses, las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Cuestionario sobre Libertad de expresión y otros derechos

Busca y pon el nombre o dirección o ejemplo concreto de cada uno de los tipos de "modos" y "medios" de comunicación en internet. Pon especial atención en aquellos que no conocías.

Internet como canal de comunicación interpersonal:

correo electrónico
listas de distribución,
grupos de noticias,
chats,
redes P2P (*peer to peer*),
foros de debate,
wikis,
juegos en red,
encuestas,
comunidades virtuales.

Internet como medio de comunicación de masas:

Páginas personales
páginas de asociaciones, instituciones y empresas,
weblogs o blogs,
portales temáticos,
buscadores y directorios
"Ciberperiodismo". Y dentro de este periodismo digital se puede distinguir entre:
-*los medios tradicionales que están en internet:*
-*medios alternativos.* En este heterogéneo grupo, podemos fijar fenómenos relativamente nuevos:

a) periódicos "confidenciales":
b) prensa fuertemente ideologizada, relativamente similar a los antiguos panfletos, pasquines y antiguas radios libres.
c) nuevos fenómenos como el periodismo "open source", fuente abierta
d) por último, dentro del periodismo digital, cabe mencionar los selectores y reproductores de información ajena : *press clipping.*

Qué nivel de protección de internet se asentó en EEUU desde 1997?

La libertad de expresión es sólo para los periodistas?

¿Crees que el anonimato en internet está, en principio protegido por algún derecho?

La libertad de expresión protege los mensajes comerciales?

Parece en las normas que se somete a internet a limitaciones más estrictas que las de otros medios de comunicación?

En términos juridicos, si Google filtra los resultados, ¿se trata de "censura"?

Qué significación básica tiene el criterio de la "relevancia pública" de la noticia?

Qué parece cambiar sobre el juicio sobre la relevancia pública?

¿Se puede seguir exigiendo diligencia y veracidad en internet? ¿Qué particulares dificultades hay?

Qué importancia puede tener extender el secreto del periodista a internet?

Crees que se ha de reconocer este derecho a los que no son "profesionales"? ¿Qué sucede en EEUU?

Sobre las posiciones críticas "libertarias" a la LSSI (www.lssice.com):

¿En el artículo "fascismo digital", que se dice a cerca de páginas-revistas como Kriptópolis?

¿En el artículo "A las armas digitales", cuáles son las tres guerras mundiales que en teoría se han librado sobre internet?

En qué aspecto se critica la inconstitucionalidad de la ley de forma concreta

Indica 6 países de los que censuran internet según el artículo
1
2
3
4
5
6

Qué situación hay en Australia

Artículo sobre responsabilidad en la web 2.0…

Qué casos de responsabilidad en internet se consideran en el texto los más polémicos? Qué causas se señalan para la atribución de la responsabilidad.

Cuál es el esquema general de responsabilidad de la Directiva europea.

Sobre qué premisas descansa el esquema de la Directiva.

Qué "anclajes" jurídicos puede tener en la LSSICE la integración de contenidos por terceros en la web 2.0.

Si no se les considera en el marco de la ley a los foro, blog, wiki, alojador de vídeos, imágenes, comentarios, etc., en qué situación queda.

Cuál es la posición del autor y de las recientes sentencias del caso mindoniense.

Qué supone la doctrina de las cartas del director, a quien se hace responsable en internet por insertar contenidos anónimamente en el caso "Mafius".

Qué supone la doctrina del reportaje neutral. Qué señala la sentencia canadiense respecto de los links.

¿Es posible aplicar pautas de diligencia al "alojador" o prestador? Que criterios se adoptaron en el caso Ramoncín. ¿Han sido mantenidos en el caso minondiense?

Qué pautas de solución se consideran por el autor, o cuales puatas de solución crees que podrían adoptarse?

Normativa sobre internet
Crees aplicable el derecho de rectificación en general en internet? Cómo crees que habría de ejercerse?

A la vista de la regulación penal de los contenidos nocivos, localiza, si tienes Internet, 5 webs que creas que vulneran dichos preceptos, pon la dirección de éstas Y SEÑALA PORQUÉ
1

2

3

4

5

LSSICE y responsabilidad por contenidos

Lee la Ley 34/2002 (en su caso acude a las preguntas y respuestas en www.lssi.es) sobre responsabilidad de contenidos y contesta a estas cuestiones:
-¿Necesito una autorización administrativa para alojar información en una web en España?

-Puedo prestar servicios de venta de objetos de culto machista?

-Si la resolución es de fuera de España, qué se ha de hacer para impedir estos contenidos prohibidos. Crees que se hace?

-Y si la cuestión afecta a un servicio de algún Estado de la Unión Europea, en caso de urgencia, ¿cuál es el procedimiento?

-¿Crees que adquiere responsabilidad una web que selecciona links de otras páginas, y recopila documentos que no son propios, si son ilícitos? Explica sobre qué base (¿es una modificación o manipulación de los datos?)

-Una página anónima recoge los datos personales de violadores condenados en España, dicha información es aprovechada por una web informativa española que recoge dicha información y la sistematiza y ordena. ¿Crees que adquiere alguna responsabilidad esta última web?

-La empresa en la que estaba alojada una web que incita a la violencia doméstica se niega a retirar los contenidos tras la petición de una Asociación de Mujeres Maltratadas. ¿Adquiere la web alguna responsabilidad disciplinaria? +

Un prestador de servicios de intermediación (ONO por ejemplo), ¿desde qué momento adquiere responsabilidad por los contenidos que permite acceder y son ilícitos?

-Qué sanción puede aplicarse al prestador de servicios que se niega retirar contenidos ilícitos en razón de la ley.

-Una web con contenidos presumiblemente ilícitos, ¿puede bloquearse provisionalmente hasta la resolución definitiva que corresponda? ¿a quién crees que suele corresponder esta competencia?

V. GENERALIDADES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y SPAM

1. Texto LSSICE respecto de cuestiones generales: definiciones, ámbito de aplicación

LEY 34/2002, DE 11 DE JULIO, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO. MODIFICADA POR LAS LEYES 32/2003, 59/2003.

ANEXO.

Definiciones

A los efectos de esta Ley, se entenderá por:

a.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. La contratación de bienes o servicios por vía electrónica.

2. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3. La gestión de compras en la red por grupos de personas.

4. El envío de comunicaciones comerciales.

5. El suministro de información por vía telemática.

6. 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:

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

8. 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.

9. 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.

10. Los servicios de radiodifusión sonora, y

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

b. 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.

c.Prestador de servicios o prestador: persona física o jurídica que proporciona un servicio de la sociedad de la información

e.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.

g. 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.

i. 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.

j. Profesión regulada: toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

l. 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.

(INCLUYE MODIFICACIONES LMISI)

TÍTULO I

Disposiciones Generales

CAPÍTULO I

Objeto

Artículo 1. Objeto.

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.

CAPÍTULO II

Ámbito de aplicación

Artículo 2. Prestadores de servicios establecidos en España.

1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

Se entenderá 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.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará 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.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador 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.

La 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.

4. 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.

Artículo 3. Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información 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 materias siguientes:

a. Derechos de propiedad intelectual o industrial.

b. Emisión de publicidad por instituciones de inversión colectiva.

c. Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d. Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

e. Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f. Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Artículo 4. Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.

A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2. (VERSIÓN ANTERIOR DECÍA 7.2 Y 8)

Los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos, además, a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables.

Artículo 5. Servicios excluidos del ámbito de aplicación de la Ley.

1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información:

a. Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.

b. Los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

2. Las disposiciones de la presente Ley, con la excepción de lo establecido en el artículo 7.1, serán aplicables a los servicios de la sociedad de la información relativos a juegos de azar que impliquen apuestas de valor económico, sin perjuicio de lo establecido en su legislación específica estatal o autonómica.

TÍTULO II
Prestación de servicios de la sociedad de la información

CAPÍTULO I
Principio de libre prestación de servicios

TÍTULO II

Prestación de servicios de la sociedad de la información

CAPÍTULO I

Principio de libre prestación de servicios

Artículo 6. No sujeción a autorización previa.

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a 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.

Artículo 7. Principio de libre prestación de servicios.

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo 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 en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

(ESTE ARTÍCULO 8 HA SIDO MODIFICADO POR LA LMISI, LA ACTUAL REDACCIÓN ES)

Artículo 8. Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) 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

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

(la versión anterior de este párrafo era: En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos

jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.)

(este apartado segundo está modificado en el sentido siguiente)

2. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

3. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

4. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

5. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.

CAPÍTULO II.
Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información

SECCIÓN I
Obligaciones

Artículo 9. Constancia registral del nombre de dominio. (DEROGADO, se incluye sólo a título informativo, para tener en cuenta que YA NO EXISTE ESTA OBLIGACIÓN)

1. Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro.

2. Los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras.

Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro.

3. La obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet.

Artículo 10. Información general.

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a. Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
b. (versión LMISI) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c. En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.
d. Si ejerce una profesión regulada deberá indicar:
    1. Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.
    2. El título académico oficial o profesional con el que cuente.
    3. El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.
    4. Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.
e. El número de identificación fiscal que le corresponda.
f. (versión LMISI) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.
g. Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. (versión LMISI) Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos 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.
e. La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el

acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

2. Preguntas y respuestas básicas generales y de interés de www.lssi.es

(Página lssi.es del Ministerio competente)

1.- ¿Quiénes están sujetos a la Ley?

Las personas que realicen actividades económicas por Internet u otros medios telemáticos (correo electrónico, televisión digital interactiva...), siempre que:

La dirección y gestión de sus negocios esté centralizada en España o,

posea una sucursal, oficina o cualquier otro tipo establecimiento permanente situado en territorio español, desde el que se dirija la prestación de servicios de la sociedad de la información.

Se presumirán establecidos en España y, por tanto, sujetos a la Ley a los prestadores de servicios que se encuentren inscritos en el Registro Mercantil o en otro Registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de un servidor situado en otro país no será motivo suficiente para descartar la sujeción a la Ley del prestador de servicios. Si las decisiones empresariales sobre el contenido o servicios ofrecidos a través de ese servidor se toman en territorio español, el prestador se reputará establecido en España.

2.- Mi empresa tiene una página web con información sobre su actividad, productos y servicios que vende, pero éstos no pueden contratarse a través de la página web, ¿me afectan las obligaciones para los prestadores de servicios?

Sí. La Ley se aplica a toda actividad con trascendencia económica que se realice por medios electrónicos. En este caso, la empresa sólo está obligada a facilitar, a través de su página web, los datos de información general establecidos en el artículo 10, que se refieren principalmente a denominación, domicilio y actividad, y a asegurarse de que la publicidad de otras empresas que, en su caso, figure en la página web pueda distinguirse claramente del contenido propio de la página y esté identificado el anunciante.

Si la empresa está inscrita en un Registro público en el que sea necesaria la inscripción para la adquisición de personalidad jurídica o a efectos de publicidad, deberá comunicar al mismo el nombre de dominio o dirección de Internet que utilice habitualmente para su identificación en Internet.

3.- ¿Los servicios que se prestan de forma gratuita están dentro del ámbito de aplicación de la Ley?

El criterio para determinar si un servicio o página web está incluido dentro del ámbito de aplicación de la Ley es si constituye o no una actividad económica para su prestador. Todos los servicios que se ofrecen a cambio de un precio o contraprestación están, por tanto, sujetos a la nueva Ley.

Sin embargo, el carácter gratuito de un servicio no determina por sí mismo que no esté sujeto a la Ley. Existen multitud de servicios gratuitos ofrecidos a través de Internet que representan una actividad económica para su prestador (publicidad, ingresos de patrocinadores, etc.) y, por lo tanto, estarían incluidos dentro de su ámbito de aplicación. Ejemplos de estos servicios serían los habituales buscadores, o servicios de enlaces y directorios de páginas web, así como páginas financiadas con publicidad o el envío de comunicaciones comerciales.

4.- ¿Cuándo se entiende que una página web representa una "actividad económica" para su titular?

Cuando éste percibe ingresos directos (por las actividades de comercio electrónico que lleve a cabo a través de la página, etc.) o indirectos (por publicidad, patrocinio, etc.) derivados de su página web, con independencia de que éstos permitan sufragar el coste de mantenimiento de la página, igualen esa cantidad o la superen.

5.- Dispongo de una página web personal. ¿Me afecta la nueva Ley?

La Ley no se aplicará a una página web personal cuando su titular no realice ningún tipo de actividad económica a través de la misma.

Si la página web tiene alojada publicidad en forma de "banners", "pop-ups", etc., su titular estará sujeto a la Ley si percibe alguna remuneración por los mismos. Si éstos no generan ningún ingreso a su titular, por ejemplo, por haber sido impuestos a cambio de la prestación de un servicio gratuito de alojamiento, éste no estará obligado a cumplir las obligaciones previstas en la Ley. Todo ello sin perjuicio de que a esa página le afecten otras normas jurídicas que sean de aplicación por ser públicamente accesible, como el Código Penal o la legislación sobre propiedad intelectual.

6.- Dispongo de una página web personal, pero para financiar gastos tengo alojados "banners" u otros medios de publicidad. ¿En qué me afecta la nueva Ley?

La Ley es de aplicación a las páginas web que ofrezcan mensajes publicitarios por los que el titular de la página perciba algún ingreso. Sin embargo, los únicos requisitos que establece la Ley en cuanto al contenido de las páginas de Internet consisten en incluir una información básica en la página web del prestador. Para una página web personal, la información que debe facilitarse es la siguiente:

a. Su nombre

b. Domicilio (indicando, al menos, la localidad y provincia de residencia)

c. Dirección de correo electrónico.

d. NIF

e. Cualquier dato que permita establecer una comunicación directa y efectiva, como podría ser, por ejemplo, un teléfono o un número de fax.

f. Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

La publicidad que se muestre en la página web deberá ajustarse a lo establecido en la Ley, la cual obliga a identificar al anunciante y a presentarla de manera claramente distinguible de los contenidos no publicitarios de la página. Así mismo, deberán respetarse las restantes normas sobre publicidad, recogidas en otras leyes.

7.- ¿Se aplica la LSSI a las Administraciones Públicas?

En general, la LSSI no se aplica a las Administraciones Públicas, puesto que éstas no tienen el carácter de prestador de servicios de la sociedad de la información definido en su anexo. De esta forma, determinadas actividades típicas de las Administraciones, como la gestión electrónica de la recaudación de tributos o la información sobre los servicios de un tercero (como podría ser la mera información en la página web de un Ayuntamiento sobre las casas rurales existentes en el término municipal) se consideran como actividades públicas o de interés general distintas a la "actividad económica" a la que se refiere la LSSI. Sin embargo, cuando la actividad de una Administración sí tenga un carácter económico (por ejemplo, la venta de libros turísticos por una entidad pública dependiente de un Ayuntamiento), le será aplicable la LSSI.

8.- ¿Es necesaria alguna autorización para prestar servicios a través de Internet?

La prestación de cualquier servicio a través de Internet u otros medios electrónicos puede realizarse libremente y no requiere ninguna autorización específica. Sin embargo, aquellas actividades o servicios que estén sujetos a autorización administrativa o a cualquier otro requisito estarán sometidos al régimen general que les sea aplicable por razón de las leyes y normas ya existentes, con independencia de que se presten a través de Internet. Por ejemplo: la autorización general de tipo C necesaria para prestar servicios de acceso a Internet seguirá siendo exigible a los proveedores de acceso a Internet y las autorizaciones precisas para la apertura de determinado tipo de establecimientos, como las farmacias, o la necesidad de colegiarse para ejercer ciertas profesiones no resultan afectadas por esta Ley.

…

12.- ¿Cuáles son las obligaciones que la Ley impone a una empresa que disponga de una página web propia a través de la que comercializa sus productos o servicios?

Las obligaciones de los prestadores de servicios que realicen actividades económicas a través de Internet se concretan en dos grupos: obligaciones de información y obligaciones en relación con la contratación on-line. Por lo que se refiere a las obligaciones de información, la empresa debe incluir en su página web información básica que permita a los usuarios identificar quién es el titular de dicha página. La información básica que se debe facilitar es, en síntesis, la siguiente:

a. Su denominación social, NIF, domicilio y dirección de correo electrónico, así como los datos de su inscripción en el Registro Mercantil, y cualquier otro dato permita una comunicación directa y efectiva, como por ejemplo un teléfono o un número de fax.

b. Información sobre el precio de los productos que ofrece, los gastos de envío y si incluye o no los impuestos aplicables.

c. Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

d. En los casos de que su actividad este sujeta a autorización previa o ejerza una profesión regulada, deberá informar a los usuarios sobre los siguientes aspectos:

a. Si ejerce alguna profesión regulada (abogado, médico, arquitecto, ingeniero), los datos básicos que acrediten su derecho a ejercer dicha profesión (título académico, colegio profesional al que pertenece).

b. Si su actividad estuviera sujeta a autorización administrativa, los datos de la autorización de que disponga.

Además de la información básica señalada anteriormente, si la empresa realiza contratos en línea o por vía electrónica a través de su página web, deberá:

a. Facilitar a los usuarios información con carácter previo al inicio de la contratación de los distintos trámites que deben seguirse para celebrar el contrato on-line,

b. Facilitar a los usuarios información sobre si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible,

c. Permitir a los usuarios la posibilidad de rectificar o corregir errores en la introducción de datos antes de confirmar el pedido,

d. Facilitar a los usuarios información con carácter previo al inicio de la contratación de la lengua o lenguas en que podrá formalizarse el contrato,

e. Poner a disposición de los usuarios, si las hubiera, las condiciones generales aplicables al contrato.

Una vez que el consumidor haya enviado su aceptación, la empresa habrá de enviarle una confirmación sobre la recepción de su pedido.

13.- ¿De qué forma ha de mostrarse la información básica sobre el prestador de servicios señalada en el artículo 10 de la Ley?

El artículo 10 de la Ley indica que la información sobre el prestador de servicios y su actividad ha de ponerse a disposición de los usuarios por medios electrónicos, de forma permanente, fácil, directa y gratuita. Cuando los servicios se prestan a través de

una página en Internet, bastará con incluir en ella esa información de manera que ésta sea accesible en la forma indicada.

Estas condiciones se cumplen cuando la información está contenida en la página de inicio del prestador de servicios o se inserta en páginas interiores relacionadas con el tipo de información de que se trate y a las que se pueda acceder a través de un enlace claramente visible, cuyo título aluda de forma inequívoca a la información de que se trate. Por ejemplo: para acceder a la información de identificación de la empresa, serviría una pestaña con el título "quiénes somos" o cualquier otro suficientemente expresivo del tipo de información a que se refiere.

3. Nueva obligación de información de seguridad

Nueva obligación introducida por la LMISI
Artículo 12 bis. Obligaciones de información sobre seguridad.

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.

4. El "spam"

Generalidades: origen, historia, importancia

http://www.rompecadenas.com.ar/sketch.htm

Sketch del spam (Monty Python's Flying Circus - 1969)

Castellano (traducción: Ana Valderrama)

Escena: Un bar. En una mesa, un grupo de Vikingos con cascos con cuernos. Un hombre y su esposa son depositados desde el techo en una mesa.

Hombre: Eric Idle

Esposa: Graham Chapman

Camarera: Terry Jones

Hombre: Sentate aquí, querida.

Esposa: Está bien.

Hombre: (a la camarera) Buen día!

Camarera: Buen día!

Hombre: Bien. ¿Qué tienen?

Camarera: Esteee... hay huevo y panceta; huevo, salchichas y panceta; huevo y spam; huevo, panceta, salchichas y spam; spam, panceta, salchichas y spam; spam, huevo, spam, spam, panceta y spam; salchichas, spam, spam, panceta, spam, tomate y spam, ...

Vikingos: (comenzando a cantar) spam, spam, spam, spam .....

Camarera: ..... spam, spam, spam, huevo y spam; spam, spam, spam, spam, spam, arvejas cocidas, spam, spam, spam.....

Vikingos: (cantando) Spam! Rico spam! Rico spam!

Camarera: .....o Langosta Termidor a la Crevette con salsa mornay a la Provenzal con cebollitas y berenjenas acompañada con paté de trufas, cognac, un huevo frito encima y spam.

Esposa: ¿Tienen algo sin spam?

Camarera: Bueno, hay spam, huevo, salchichas y spam, que no tiene mucho spam.

Esposa: No quiero nada de spam!

Hombre: ¿Por qué no le trae huevo, panceta, spam y salchichas?

Esposa: Porque tiene spam!

Hombre: Pero no tiene tanto como el spam, huevo, salchichas y spam, no?

Vikingos: spam, spam, spam, spam ("in crescendo" durante las siguientes frases de la conversación)

Esposa: ¿Podría preparar huevo, panceta, spam y salchichas sin spam, entonces?

Camarera: Urgghh!

Esposa: ¿Qué quiere decir con "Urgghh!"? No me gusta el spam!

Vikingos: Rico spam! Maravilloso spam!

Camarera: Cállense!

Vikingos: Rico spam! Maravilloso spam!

Camarera: Cállense! (los Vikingos se detienen) Malditos Vikingos! No, no puede pedir huevo, panceta y salchichas sin spam.

Esposa: (chilla) No me gusta el spam!

Hombre: Shhh, querida, no hagas un escándalo. Yo me comeré tu spam. Me encanta. Y voy a pedir spam, spam, spam, spam, spam, spam, spam, arvejas cocidas, spam, spam, spam y spam!

Vikingos: (cantando) Spam, spam, spam, spam. Rico spam! Maravilloso spam!

Camarera: Cállense! No nos quedaron arvejas.

Hombre: Bueno, ¿podría comer el spam de ella en lugar de las arvejas, entonces?

Camarera: Quiere decir spam, spam, spam, spam, spam, spam, spam .... (pero es demasiado tarde, y el canto de los Vikingos ahoga el sonido de sus palabras)

Vikingos: Spam, spam, spam, spam. Rico spam! Maravilloso spam! Spam, spa-a-a-a-a-am, spa-a-a-a-a-am, spam. Rico spam! Rico spam! Rico spam! Rico spam! Rico spam! Spam, spam, spam, spam.

De

http://www.telecable.es/personales/carlosmg1/spam_historia.htm

¿Qué es el spam?

Pero, por lo que a nosotros respecta, SPAM es la expresión con la que se conoce el correo no solicitado, es decir, los mensajes que nos envían a nuestro buzón, sin que nosotros hayamos pedido que nos los enviaran.

El diccionario Merriam-Webster recoge el término spam:

Etymology: from a skit on the British television series Monty Python's Flying Circus in which chanting of the word Spam (trademark for a canned meat product) overrides the other dialogue.Date: 1994: unsolicited usually commercial E-mail sent to a large number of addresses.

Algunos datos sobre el SPAM

Fuentes diversas. Los datos varían mucho según fuentes.

En 2006, los usuarios de informática se gastaron un total de 6.000 millones de euros en reparar y reemplazar ordenadores infectados por correo basura o "spam", según un estudio difundido hoy por Deloitte.

El 'spam' supuso en 2006 el 95% de los mails enviados en todo el mundo, y en la actualidad, cada día se envían 60.000 millones de e-mails catalogados como correo basura.

Volumen (Algunos números):

A principio de 2005, el 80% del tráfico de e-mails a nivel mundial era spam.

Actualmente se envían 500 millones de e-mails diarios clasificables como "spam" según la consultora Prince&Cooke

El 23,1% proviene de computadoras de EE.UU. y un 21,9%, de China.

Más del 70% del spam se envía desde computadoras "zombies", ordenadores infectados que van reenviando spam sin que sus propietarios lo sepan.

España es el quinto productor de correo basura en el mundo

Trend Argentina dio a conocer un estudio donde se informa que el envío de e-mail con publicidad no solicitada en español creció un 42 por ciento en el primer trimestre de 2007 y los expertos advierten que seguirá aumentando.

Costes económicos:

Según AOL, mayor proveedor mundial de acceso a la red, el spam llegó a representar un 83% del tráfico informático en el peor momento de este año y ha costado a los proveedores de Internet alrededor de 500 millones de dólares (unos 360 millones de euros) en banda ancha desperdiciada.

Otros datos: 2005 se dijo: las empresas necesitan entre 15 y 20 minutos por empleado al día para eliminar este tipo de publicidad, lo que supone "miles de millones de euros perdidos en productividad". Según los datos de 2002, el spam ha costado a las empresas de la Unión Europea aproximadamente 2.500 millones de euros en pérdidas. El 80% de spam incluye además un 80% de correos electrónicos claramente ilegales, mientras que el restante 20% no está perfectamente tipificado, sino que es dudoso.

Tratamiento del SPAM en la LSSICE

TÍTULO III

Comunicaciones comerciales por vía electrónica

Artículo 19. Régimen jurídico.

1. Las comunicaciones comerciales y las ofertas promocionales se regirán además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Artículo 20, nueva redacción LMISI

Artículo 20. Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi". *(antes sólo "publicidad")*

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

Lo siguiente es nuevo:

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Artículo 22. Derechos de los destinatarios de servicios.

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. 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.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

La Ley (artículo 38.3.C) señala como infracción grave

c) 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 en el artículo 21.

y sanciona (en el artículo 38.3.c) como infracciones leves

d)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 en el artículo 21 y no constituya infracción grave.

y (artículo 38.4)

Artículo 39. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

Prohibición parece que va más allá de los mensajes "comerciales"

No se olvide que la prohibición viene referida a comunicaciones "comerciales" "publicitarias" o "promocionales" no solicitadas (art. 21). Pero, aunque aún no se conoce resolución judicial al respecto, órganos especializados y muy autorizados consideran que la prohibición sí que alcanza también a la comunicación de organizaciones sin ánimo de lucro y políticas[64]. Ya se ha dado algún caso de inspección y actuación de la AGPD por denuncia de envíos de correo electrónico para pedir votos en elecciones universitarias.

Mail como dato personal, spam desde la perspectiva de la protección de datos.

Desde la Memoria anual de la AGPD de 1999, esta institución así considera, en principio, con relación a las cuentas conformadas con nombres o apellidos del usuario.

De este modo, el tratamiento de estos datos personales y su obtención para luego remitir spam está sujeto al régimen de la ley: consentimiento, información, principios, cesión, etc. Por todo ello, al remitir spam puedes estar probando que dispones ilícitamente de mails y los has tratado. En su caso, puedes estar probando que aun teniéndolos lícitamente, los usas fuera de las finalidades legítimas.

Sanción AGPD por mandar a muchos mails y dejarlos visibles

Además de las posibles infracciones de la LSSICE, al tratarse de dato personal, pero todo aquel que en una actividad que no sea doméstica o personal deje a la vista las direcciones de correo electrónico de sus destinatarios está cometiendo una infracción multada hasta con 60.101, 21 euros por la Ley Orgánica de Protección de Datos (LOPD).

Así, según noticia de *El País* de febrero de 2007, se comenta que Dª A.G. S. sabe bien que no se trata de una amenaza, pues ha tenido que pagar 601,01 euros por haber dejado a la vista 42 direcciones de email al enviar un mensaje promocional de telefonía móvil por encargo de una pequeña empresa conocida como La Cremallera, que estaba llevando a cabo una campaña para Vodafone.

Uno de los destinatarios de este mensaje sintió que se violaba su intimidad al exponer su dirección y no utilizar la opción de copia oculta (CCO), y presentó una denuncia ante la Agencia Española de Protección de Datos (AEPD), quien inició el proceso.

---

64 Grupo del artículo 29 en el ámbito europeo, "la prohibición de SPAM alcanza toda forma de promoción de ventas, incluido el marketing directo por organizaciones de caridad y organizaciones políticas". Así, en la Opinión 5/2004, de 27 de enero, sobre comunicaciones comerciales no solicitadas, pág.7.

Cuestionario sobre Cuestiones generales LSSICE: prestación de servicios

LSSICE (la respuesta a muchas cuestiones la tendrá más clara al ver el texto de la ley y también en preguntas y respuestas sobre la LSSI).

Las cuestiones concretas de comercio electrónico han de ser analizadas con la normativa especial de contratación electrónica.

-Anexo con definiciones:

¿Cuál es el concepto básico de servicio de la sociedad de la información (SSI)?

¿Puede ser un SSI una página personal donde hable de mí y de mis gustos?

¿Es un SSI enviar publicidad a correos electrónicos?

¿Es un SSI que un profesor de la Universidad envíe información sobre un curso relativo a la asignatura?

Es un SSI la cadena Ser cuando emite por internet?

Qué es un servicios de intermediación (anexo) en general?

Crees que esta ley está pensada para la web social en la que todos integran contenidos (enlaces, vídeos, texto, etc.) en los sitios de otros (foros, wikis, youtube, etc.). El foro que esos contenidos de terceros es un prestador de servicios de intermediación o simplemente un prestador de servicios de la sociedad de la información?

Texto de la ley, cuestiones generales

¿Cuándo se entiende que un prestador de servicios de la sociedad de la información (PSSI) está establecido en España y, por tanto, sometido a la ley?

Mi empresa está radicada legalmente en la Isla de Tuvalú, pero la dirección la llevo desde Sant Sadurní de Noia, ¿estoy sometido a la ley, porqué?

Trabajo en España para "Boston Trade", multinacional con sede en España, ¿se me aplica la ley, por qué?, ¿Se le aplica a Boston-Trade, en Chile, por tener sede en España?

Se aplica la ley española a una Financiera Francesa que realiza comunicaciones comerciales electrónicas en España?

Una empresa establecida en Holanda que vende a los consumidores finales zapatillas de deporte ¿está sometida a la LSSICE si vende a españoles en España?

¿Necesito una autorización previa para tener mi página web personal con publicidad?

¿Necesita una farmacia autorización previa para poder comerciar electrónicamente?

Dado que se afirma el principio de no sujeción a autorización previa, ¿puedo montar una farmacia por internet?

Respecto de todo PSSI, prestador de servicios que venda, tenga en cuenta lo que se dirá en el ámbito de la Ley de comercio minorista.

Ha superado los estudios en la Universidad, se hace un profesional, dado de alta en su caso en el Colegio correspondiente, en su página web ofrece sus servicios y permite su prestación por medios electrónicos. Por favor complemente todas las exigencias del artículo 10, como si escribiera el apartado "Sobre nosotros" o "Quienes somos" en su web.

¿Qué se puede hacer respecto de un un PSSI que incumple los principios del artículo 8 y que descubrimos que está establecido en Austria?

¿Qué se puede hacer respecto de un un PSSI que incumple los principios del artículo 8 y que descubrimos que está establecido en Australia (art. 11)?

<u>Nueva obligación de información de seguridad artículo 12 bis:</u>

Cuál es el ámbito de aplicación de esta nueva obligación (recuerda el concepto de PSI). ¿Crees que sólo hace referencia a los operadores de telecomunicaciones?

¿Si tu empresa facilita servicios de correo electrónico, queda obligada por esta norma?

¿Si se utilizan filtros de SPAM en el mail, hay que informar al respecto de los mismos al usuario? ¿Dónde, con qué requisitos generales?

Intenta localizar esta información obligatoria en algún serivicio de correo electrónico y pon la información aquí:

LSSICE-SPAM

- De dónde proviene el término "spam"

-Qué es el spam

Datos sobre el spam:

Cuántos millones de euros se calcula que se gastan en reparar y reemplazarordenadores infectados por spam?

Qué porcentaje de mails se calcula que son spam.

Cuántos millones de mails se consideran spam, observe disparidad de datos.

Procedencia del spam por países?

Desde dónde se envía el 70% del spam?

Que porcentaje del tráfico informático se considera que representa el spam.

En millones de dólares de banda ancha desperdiciada cuánto se calcula el coste?

Desde la perspectiva del tiempo de trabajo desperdiciado cuánto se supone que perdieron las empresas europeas en 2002?

Qué conexión suele haber entre los mensajes basura y la ilegalidad del contenido de éstos?

Tratamiento en la LSSICE

Observe que el envío de mensajes comerciales no sólo se regula por esta ley, sino por la normativa específica y la que afecte, por ejemplo, por protección del derecho a la protección de datos personales.

Qué requisitos ha de tener según el artículo 20. 1º una comunicación electrónica, qué palabra ha de figurar?

Para remitir una comunicación electrónica qué requisitos generales deben cumplirse. (art. 21. 1).

En una Agencia de viajes contrato un viaje, me pidieron el mail para confirmar algunos datos del viaje. ¿Puede remitirme posteriormente publicidad sobre otros viajes?

Compré un billete de avión por una web, desde entonces recibo ofertas promocionales de esa página web en mi correo electrónico. Es legal? (art. 21. 2º)

Aunque sea legal el envío de mensajes comerciales, ¿es posible solicitar no publicidad en tu correo electrónico? ¿Cómo hacerlo según la ley?

-¿Qué sanción puede tener quien remita más de tres correos no deseados sin solicitud o autorización alguna?

Puedo usar mails obtenidos de directorios de empresas o instituciones en internet para remitir información en contra de la guerra, la paz en el mundo, o la

religión que profeso, sin pretender obtener ningún donativo, remuneración, etc.?

En el directorio de una empresa o de una universidad encuentro los mails de su personal puesto que están accesibles…Puedo hacer una base de datos con tales mails, según procedencias, etc.?

Qué puede pasar si remito un mail a muchas cuentas de correos y no es personal sin utilizar la copia de carbón oculta (CCO:), es decir, mando a una lista de correo bien en el campo "Para:" o "CC:"?

Preguntas sobre "Preguntas y respuestas LSSI" sobre cuestiones generales (NO repita lo que dice el texto)

De Preguntas y respuestas LSSICE

¿La utilización de un servidor situado en otro país sirve para eludir la aplicación de la ley?

¿Se aplica la ley aunque la web de la empresa no sea para contratar o comerciar electrónicamente?

Los servicios de la web son gratuitos, ¿Se aplica la ley?

¿Se aplica la Ley a un blog personal?

¿Se aplica la ley a la venta de camisetas de "Valencia" en la web del Ayuntamiento de Valencia?

Crees que se aplica el sistema de responsabilidad de los ISP y PSSI a las administraciones públicas. Razona tu respuesta.

¿Cómo tiene que disponerse la información obligatoria del artículo 10?

¿Qué implica la presunción sobre el lugar de celebración del contrato electrónico establecida en el artículo 29 de la Ley?

¿Se aplica la legislación española si un consumidor residente en España compra un producto o contrata un servicio a una tienda on-line extranjera?

VI. COMERCIO Y CONTRATACIÓN ELECTRÓNICA

Recurso sobre e-comercio muy recomendable

Buscar: "Marco jurídico español del comercio electrónico" "Eugenio Ribón"

http://cec.consumo-inc.es/cec/secciones/Actividades/Eventos/Ponencias_Bilbao/MARCO_JURIDICO_ESPANOL_DEL_COMERCIO_ELECTRONICO_PARA_CEC.pdf

1.Jurisdicción general aplicable en contratación

Ley orgánica poder judicial, regla general:

Artículo 22

En el orden civil, los Juzgados y Tribunales españoles serán competentes:

2. Con carácter general, cuando las partes se hayan sometido expresa o tácitamente a los Juzgados o Tribunales españoles, así como cuando el demandado tenga su domicilio en España.

…

4. Asimismo, en materia de contratos de consumidores, cuando el comprador tenga su domicilio en España si se trata de una venta a plazos de objetos muebles corporales o de préstamos destinados a financiar su adquisición; y en el caso de cualquier otro contrato de prestación de servicio o relativo a bienes muebles, cuando la celebración del contrato hubiere sido precedida por oferta personal o de publicidad realizada en España o el consumidor hubiera llevado a cabo en territorio español los actos necesarios para la celebración del contrato; en materia de seguros, cuando el asegurado y asegurador tengan su domicilio habitual en España; y en los litigios relativos a la explotación de una sucursal, agencia o establecimiento mercantil, cuando éste se encuentre en territorio español. En materia concursal se estará a lo dispuesto en su ley reguladora.

www.lssi.es

18.- Si tengo algún problema con la compra realizada por Internet o correo electrónico con un prestador de otro país, ¿puedo acudir a los tribunales españoles?

Para determinar la jurisdicción competente para la resolución de conflictos en materia contractual cuando un consumidor intervenga como parte en el contrato, es preciso acudir a las normas de Derecho Internacional privado, las cuales tienen en cuenta distintos puntos de conexión para fijar la extensión de la jurisdicción de los jueces y tribunales.

Con carácter general, un consumidor residente en España que haya celebrado un contrato on-line con un prestador establecido fuera de España sólo podrá ser demandado ante los tribunales españoles y podrá, a su vez, demandar al prestador ante los tribunales españoles cuando el contrato se haya celebrado gracias a una oferta que el prestador le hubiera dirigido personalmente (correo electrónico) o que hubiera dirigido al mercado español o a varios mercados, incluido el español.

En los demás casos, si un consumidor residente en España quisiera demandar a una empresa establecida fuera de nuestro país por el incumplimiento de un contrato celebrado por vía electrónica, sería necesario alegar otras circunstancias, por ejemplo, que la obligación que da lugar a la demanda debía cumplirse en España, para fundar la competencia de los tribunales españoles.

Como se ve, en la contratación transfronteriza, no siempre puede asegurarse que los jueces y tribunales españoles sean competentes para conocer de la demanda. Por eso, la Ley potencia los mecanismos de resolución extrajudicial de conflictos, y, en especial, aquéllos que se basen en la utilización de medios electrónicos y sean reconocidos en otros Estados.

2.Ley aplicable en contratación electrónica

(aunque suele estar relacionado, recuerde que una cosa es la norma aplicable y otra la jurisdicción a la que acudir, pudiéndose dar el caso de que el juez de un país deba aplicar la normativa de otro país).

Regla general Código civil

Según el artículo 10 del Código Civil y como regla general

Señale por el orden aplicable qué ley se aplica en el ámbito de contratos, piense su aplicabilidad a internet:

1º la pactada.

2º ley nacional común

3º residencia común

4º lugar del contrato

Artículo 10.

5. Se aplicará a las obligaciones contractuales la ley a que las partes se hayan sometido expresamente, siempre que tenga alguna conexión con el negocio de que se trate; en su defecto, la ley nacional común a las partes; a falta de ella, la de la residencia habitual común, y, en último término, la ley del lugar de celebración del contrato.

Para el caso de Unión Europea y Espacio económico europeo, tenga en cuenta el Convenio de Roma de 1980.

Tenga en cuenta que la elección de ley aplicable no puede privar de la protección de las leyes del país de residencia del consumidor en diversos casos.

Piense en una página web de la que se intuye que va dirigida al consumidor español.

Que se hubiera recibido correo electrónico por el vendedor extranjero.

Si en todo caso se hace un pedido –específico- y el vendedor lo tramita.

En todo caso, se rige por régimen específico lo relativo a transporte, servicios a prestar en lugar diferente de residencia (pensemos en hoteles, turismo, etc.).

CONVENIO SOBRE LA LEY APLICABLE A LAS OBLIGACIONES CONTRACTUALES abierto a la firma en Roma el 19 de junio de 1980 (80/934/CEE)

Versión 2008

"1. Los contratos de consumo en el sentido y en las condiciones previstos en el apartado siguiente se regirán por la ley del Estado miembro en que el consumidor tenga su residencia habitual.

2. El apartado 1 se aplicará a los contratos celebrados por una persona física, el consumidor, que tenga su residencia habitual en un Estado miembro, para un uso que pueda considerarse ajeno a su actividad profesional, con otra persona, el profesional, que actúe en ejercicio de su actividad profesional.

Se aplicará siempre que el contrato haya sido celebrado con un profesional que ejerza actividades comerciales o profesionales en el Estado miembro de la residencia habitual del consumidor o que, por cualquier medio, dirija estas actividades a dicho Estado o a varios países entre los que se cuente dicho Estado miembro, y que el contrato esté comprendido en el marco de dichas actividades, a menos que el profesional ignore el lugar de la residencia habitual del consumidor y que esta ignorancia no sea imputable a una imprudencia por su parte.

3. El apartado 1 no se aplicará a los siguientes contratos:

(a) contratos de suministro de servicios cuando los servicios deban prestarse al consumidor, exclusivamente, en un país distinto de aquel en que tenga su residencia habitual;

(b) contratos de transporte que no se refieran a un viaje combinado con arreglo a la definición de la Directiva 90/314/CEE, de 13 de junio de 1990;

(c) contratos que tengan por objeto un derecho real inmobiliario o un derecho de uso de un edificio que no tengan por objeto un derecho de utilización en régimen de tiempo compartido con arreglo a la definición de la Directiva 94/47/CE, de 26 de octubre de 1994."

[El texto del artículo 6 la versión de 2008 es el que sigue :]

¡Artículo 6 Contratos de consumo

1. Sin perjuicio de los artículos 5 y 7, el contrato celebrado por una persona física para un uso que pueda considerarse ajeno a su actividad profesional o profesión ("el consumidor") con otra persona ("el profesional") que actúe en ejercicio de su actividad profesional o profesión, se regirá por la ley del país en que el consumidor tenga su residencia habitual, a condición de que:

a) desempeñe sus actividades comerciales o profesionales en el país donde el consumidor tenga su residencia habitual, o b) dirija estas actividades de algún modo a ese país o a distintos países, incluido ese país, y el contrato entre en el ámbito de dichas actividades.

2. Sin perjuicio del apartado 1, las partes podrán elegir la ley aplicable a un contrato que cumple los requisitos del apartado 1, de conformidad con el artículo 3. No obstante, dicha elección no podrá acarrear, para el consumidor, la pérdida de la protección que le proporcionen aquellas disposiciones inalienables por contrato en virtud de la ley que, a falta de elección, habrían sido aplicables en virtud del apartado 1.

3. En caso de incumplimiento de las condiciones recogidas en las letras a) y b) del apartado 1, la ley aplicable a un contrato entre un consumidor y un profesional se determinará de conformidad con los artículos 3 y 4.

4. Los apartados 1 y 2 no se aplicarán a los siguientes contratos:

a) contratos de suministro de servicios cuando los servicios deban prestarse al consumidor, exclusivamente, en un país distinto de aquel en que tenga su residencia habitual;

b) contratos de transporte que no se refieran a un contrato relativo a un viaje combinado con arreglo a la definición de la Directiva 90/314/CEE del Consejo, de 13 de junio de 1990, relativa a los viajes combinados, las vacaciones combinadas y los circuitos combinados;

c) contratos que tengan por objeto un derecho real inmobiliario o al alquiler de un edificio que no tengan por objeto un contrato relativo al derecho inmobiliario de utilización en régimen de tiempo compartido con arreglo a la definición de la Directiva 94/47/CE;

d) derechos y obligaciones que constituyan un instrumento financiero y derechos y obligaciones que constituyan los términos y condiciones que regulan la emisión, la oferta al público o las ofertas públicas de emisión de valores negociables, y la suscripción y el reembolso de participaciones en organismos de inversión colectiva, siempre y cuando no constituyan la prestación de un servicio financiero;

e) los contratos celebrados con un tipo de sistema que entre dentro del ámbito de aplicación del artículo 4, apartado 1, letra h).

LSSICE

Artículo 3. Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información 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 materias siguientes:

…d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

Artículo 26. Ley aplicable.

Para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español, debiendo tomarse en consideración para su aplicación lo establecido en los artículos 2 y 3 de esta Ley.

VER LUGAR DE CONTRATO

Contestaciones www.lssi.es

17.- ¿Se aplica la legislación española si un consumidor residente en España compra un producto o contrata un servicio a una tienda on-line extranjera?

La normativa española se aplicará a los contratos que los consumidores celebren con prestadores establecidos en España. El lugar de establecimiento en España de un prestador de servicios debe estar indicado en su página web y puede comprobarse mediante consulta al Registro Mercantil u otro en que el prestador esté inscrito.

También se aplicará la Ley española a las compras que efectúen a prestadores de servicios establecidos en otro Estado de la Unión Europea o del Espacio Económico Europeo (países de la Unión Europea más Noruega, Islandia y Liechtenstein), siempre que la normativa española sea más beneficiosa para el consumidor que la legislación del país en que resida el prestador de servicios.

Si la compra o la contratación del servicio se realiza a un prestador de servicios establecido en un país que no pertenezca al Espacio Económico Europeo, la legislación española sólo será aplicable si los consumidores españoles compran en tiendas virtuales que dirijan su actividad al mercado español o se hayan puesto en contacto con el consumidor a través de correo electrónico.

3.LSSICE y e-contratación

Regulación general contratación electrónica LSSICE

TÍTULO IV

Contratación por vía electrónica

Artículo 23. Validez y eficacia de los contratos celebrados por vía electrónica.

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

Artículo 24. Prueba de los contratos celebrados por vía electrónica.

1. VERSIÓN LMISI La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

Artículo 25. Intervención de terceros de confianza.

1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

artículo 1.262 del Código Civil, que queda redactado de la siguiente manera:

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 que se hizo la oferta.

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

artículo 54 del Código de Comercio

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 que se hizo la oferta.

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

(ley comercio minorista)

Artículo 41. Necesidad de consentimiento expreso.

1. En ningún caso la falta de respuesta a la oferta de venta a distancia podrá considerarse como aceptación de ésta.

2. Si el vendedor, sin aceptación explícita del destinatario de la oferta, enviase a éste el producto ofertado, se aplicará lo dispuesto en el artículo siguiente.

(NO olvide en todo caso nulidades y causas de desistimiento o resolución del contrato de venta a distancia…)

LSSICE Artículo 28. Información posterior a la celebración del contrato. (ver en contratación LSSICE)

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a.El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o

b. La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante

haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.

2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.

En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquel haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a.Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b. El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

Continúa LSSICE

Artículo 29. Lugar de celebración del contrato.

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

…

CAPÍTULO II

Solución extrajudicial de conflictos

Artículo 32. Solución extrajudicial de conflictos.

1. El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos, en los términos que establezca su normativa específica.

(AL RESPECTO DE ARBITRAJE, a título informativo, TENGA EN CUENTA LA RECIENTE REGULACIÓN LEGAL Y REGLAMENTARIA: Real Decreto 231/2008, de 15 de febrero, por el que se regula el Sistema Arbitral de Consumo)

4.LMISI 2007: obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
Jefatura del Estado (BOE n. 312 de 29/12/2007, páginas: 53701 - 53719
Artículo 2. Obligación de

1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.

b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.

c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.

d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

2. A los efectos de lo dispuesto en el apartado anterior, tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica, las que agrupen a más de cien trabajadores o su volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.010.121,04 euros y que, en ambos casos, operen en los siguientes sectores económicos:

a) Servicios de comunicaciones electrónicas a consumidores, en los términos definidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

b) Servicios financieros destinados a consumidores, que incluirán los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros. En particular, se entenderá por:

1. Servicios bancarios, de crédito o de pago: las actividades relacionadas en el artículo 52 de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito.

2. Servicios de inversión: los definidos como tales en la Ley 24/1988, de 28 de julio, del Mercado de Valores.

3. Operaciones de seguros privados: las definidas en el artículo 3 del texto refundido de la Ley de ordenación y supervisión de los seguros privados, aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre.

4. Planes de pensiones: los definidos en el artículo 1 del texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre.

5. Actividad de corredor de seguros: la definida en la Ley 26/2006, de 17 de julio, de mediación en seguros y reaseguros privados.

c) Servicios de suministro de agua a consumidores, definidos de acuerdo con la normativa específica.

d) Servicios de suministro de gas al por menor, de acuerdo con lo dispuesto en la Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.

e) Servicios de suministro eléctrico a consumidores finales, de acuerdo con lo dispuesto en el título VIII de la Ley 54/1997, de 27 noviembre, del Sector Eléctrico.

f) Servicios de agencia de viajes, de acuerdo con lo dispuesto en el Real Decreto 271/1988, de 25 de marzo, por el que se regula el ejercicio de las actividades propias de las agencias de viajes.

g) Servicios de transporte de viajeros por carretera, ferrocarril, por vía marítima, o por vía aérea, de acuerdo con lo dispuesto en la normativa específica aplicable.

h) Actividades de comercio al por menor, en los términos fijados en el apartado 2 del artículo 1 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista y en su normativa de desarrollo, a las que serán de aplicación únicamente los apartados c) y d) del apartado 1 del presente artículo.

3. Excepcionalmente, el Gobierno o, en su caso, los órganos competentes de las Comunidades Autónomas podrán ampliar el ámbito de aplicación del apartado 1 del presente artículo a otras empresas diferentes de las previstas en la Ley, en aquellos casos en los que, por la naturaleza del servicio que presten, se considere que en el desarrollo de su actividad normal deban tener una interlocución telemática con sus clientes o usuarios.

En el plazo de un año desde la entrada en vigor de la obligación a que se refiere el apartado 1, el Gobierno analizará la aplicación del apartado 2 de este artículo a otras empresas con más de cien trabajadores o que tengan un volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, superior a 6.010.212,04 euros, que en el desarrollo de su actividad normal, presten servicios en los que se considere que deban tener una interlocución telemática con sus clientes o usuarios.

Las Comunidades Autónomas con competencias exclusivas en las materias objeto de obligación de comunicación telemática podrán modificar el ámbito y la intensidad

de aplicación del apartado 1 del presente artículo en aquellos casos en que precisamente debido al desarrollo sectorial de sus competencias lo consideren oportuno.

5. Información general, contratación y ventas

Se recopilan algunas obligaciones de información de LSSICE, Ley de comercio minotista, Ley condiciones generales de contratación, etc. de especial interés para todo prestador de servicios que efectúe contratación a distancia.

Haya o no contratación no hay que olvidar la información general del artículo 10 LSSICE, que también se da cuando hay contratación. No se olvide que si la contratación consumo, concurren las obligaciones de consumo, y si es venta, las de venta a distancia. Habría que sumar todas las obligaciones específicas para ámbitos concretos que puedan darse.

LSSICE

VERSIÓN LMISI 2007

ART. 27 (VER INFORMACIÓN CONTRATACIÓN)

Artículo 27. Obligaciones previas a la contratación.

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación *de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre 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.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior *se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.*

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.

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.

TÍTULO VI

Información y control

Versión LMISI 2007

Artículo 33. Información a los destinatarios y prestadores de servicios.

Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.

Artículo 34. Comunicación de resoluciones relevantes.

1. El Consejo General del Poder Judicial remitirá al Ministerio de Justicia, en la forma y con la periodicidad que se acuerde mediante Convenio entre ambos órganos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y los prestadores de servicios de la sociedad de la información.

2. Los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos a que se refiere el artículo 32.1 comunicarán al Ministerio de Justicia los laudos o decisiones que revistan importancia para la

prestación de servicios de la sociedad de la información y el comercio electrónico de acuerdo con los criterios indicados en el apartado anterior.

3. En la comunicación de las resoluciones, laudos y decisiones a que se refiere este artículo, se tomarán las precauciones necesarias para salvaguardar el derecho a la intimidad y a la protección de los datos personales de las personas identificadas en ellos.

4. El Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso de cualquier interesado a la información recibida de conformidad con este artículo.

Información Condiciones Generales de Contratación Ley 7/1998sobre condiciones generales de la contratación.

Artículo 5. Requisitos de incorporación.

1. Las condiciones generales pasarán a formar parte del contrato cuando se acepte por el adherente su incorporación al mismo y sea firmado por todos los contratantes. Todo contrato deberá hacer referencia a las condiciones generales incorporadas.

No podrá entenderse que ha habido aceptación de la incorporación de las condiciones generales al contrato cuando el predisponente no haya informado expresamente al adherente acerca de su existencia y no le haya facilitado un ejemplar de las mismas.

…

3. En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.

4. La redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez.

Real Decreto 1906/1999

Artículo 2. Deber de información previa

Previamente a la celebración del contrato y con la antelación necesaria, como mínimo en los tres días naturales anteriores a aquélla, el predisponente deberá facilitar al adherente, de modo veraz, eficaz y completo, información sobre todas y cada una de las cláusulas del contrato y remitirle, por cualquier medio adecuado a la técnica de comunicación a distancia utilizada, el texto completo de las condiciones generales.

6. Información artículo 47 en Ley 7/1996, de 15 de enero, de Ordenación del comercio minorista

(y tenga en cuenta las posibilidades de resolución y consecuencias por falta de información, así como la prueba de la información).

Artículo 40. Información previa.

1. Antes de iniciar el procedimiento de contratación y con la antelación necesaria, el vendedor deberá suministrar al consumidor, de forma veraz, eficaz y suficiente, la siguiente información:

La identidad del vendedor y su dirección.

Las características esenciales del producto.

El precio, incluidos todos los impuestos.

Los gastos de entrega y transporte, en su caso.

La forma de pago y modalidades de entrega o de ejecución.

La existencia de un derecho de desistimiento o resolución, o su ausencia en los contratos a que se refiere el artículo 45.

El coste de la utilización de la técnica de comunicación a distancia cuando se calcule sobre una base distinta de la tarifa básica.

El plazo de validez de la oferta y del precio.

La duración mínima del contrato, si procede, cuando se trate de contratos de suministro de productos destinados a su ejecución permanente o repetida.

Las circunstancias y condiciones en que el vendedor podría suministrar un producto de calidad y precio equivalentes, en sustitución del solicitado por el consumidor, cuando se quiera prever esta posibilidad.

En su caso, indicación de si el vendedor dispone o está adherido a algún procedimiento extrajudicial de solución de conflictos.

2. La información contenida en el apartado anterior, cuya finalidad comercial debe ser indudable, deberá facilitarse al comprador de modo claro, comprensible e inequívoco, mediante cualquier técnica adecuada al medio de comunicación a distancia utilizado, y deberá respetar, en particular, el principio de buena fe en las transacciones comerciales, así como los principios de protección de quienes sean incapaces de contratar.

Artículo 47. Información. 1. Además de la información señalada en el artículo 40, el consumidor deberá haber recibido, a la ejecución del contrato, las siguientes informaciones y documentos:

Información escrita sobre las condiciones y modalidades de ejercicio de los derechos de desistimiento y resolución, así como un documento de desistimiento o revocación, identificado claramente como tal, que exprese el nombre y dirección de la

persona a quien debe enviarse y los datos de identificación del contrato y de los contratantes a que se refiere.

La dirección del establecimiento del vendedor donde el comprador pueda presentar sus reclamaciones.

Información relativa a los servicios postventa y a las garantías comerciales existentes.

En caso de celebración de un contrato de duración indeterminada o de duración superior a un año, las condiciones de rescisión del contrato.

2. La información a que se refiere el apartado anterior deberá facilitarse por escrito o, salvo oposición expresa del consumidor, en cualquier otro soporte duradero adecuado a la técnica de comunicación empleada y en la lengua utilizada en la propuesta de contratación.

7. Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación: cláusulas de la contratación, información y vinculación

Artículo 1. Ámbito objetivo.

1. 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.

2. El hecho de que ciertos elementos de una cláusula o que una o varias cláusulas aisladas se hayan negociado individualmente no excluirá la aplicación de esta Ley al resto del contrato si la apreciación global lleva a la conclusión de que se trata de un contrato de adhesión.

…

Artículo 5. Requisitos de incorporación.

1. Las condiciones generales pasarán a formar parte del contrato cuando se acepte por el adherente su incorporación al mismo y sea firmado por todos los contratantes. Todo contrato deberá hacer referencia a las condiciones generales incorporadas.

No podrá entenderse que ha habido aceptación de la incorporación de las condiciones generales al contrato cuando el predisponente no haya informado expresamente al adherente acerca de su existencia y no le haya facilitado un ejemplar de las mismas.

…

3. En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada

una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.

4. La redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez.

Artículo 6. Reglas de interpretación.

1. Cuando exista contradicción entre las condiciones generales y las condiciones particulares específicamente previstas para ese contrato, prevalecerán éstas sobre aquéllas, salvo que las condiciones generales resulten más beneficiosas para el adherente que las condiciones particulares.

2. Las dudas en la interpretación de las condiciones generales oscuras se resolverán a favor del adherente. En los contratos con consumidores esta norma de interpretación sólo será aplicable cuando se ejerciten acciones individuales.

3. Sin perjuicio de lo establecido en el presente artículo, y en lo no previsto en el mismo, serán de aplicación las disposiciones del Código Civil sobre la interpretación de los contratos.

CAPÍTULO II.

No incorporación y nulidad de determinadas condiciones generales.

Artículo 7. No incorporación.

No quedarán incorporadas al contrato las siguientes condiciones generales:

Las que el adherente no haya tenido oportunidad real de conocer de manera completa al tiempo de la celebración del contrato o cuando no hayan sido firmadas, cuando sea necesario, en los términos resultantes del artículo 5.

Las que sean ilegibles, ambiguas, oscuras e incomprensibles, salvo, en cuanto a estas últimas, que hubieren sido expresamente aceptadas por escrito por el adherente y se ajusten a la normativa específica que discipline en su ámbito la necesaria transparencia de las cláusulas contenidas en el contrato.

Artículo 8. Nulidad.

1. Serán nulas de pleno derecho las condiciones generales que contradigan en perjuicio del adherente lo dispuesto en esta Ley o en cualquier otra norma imperativa o prohibitiva, salvo que en ellas se establezca un efecto distinto para el caso de contravención.

2. En particular, serán nulas las condiciones generales que sean abusivas, cuando el contrato se haya celebrado con un consumidor, entendiendo por tales en todo caso las definidas en el artículo 10 bis y disposición adicional primera de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

TENGA EN CUENTA QUE EN ESTA LEY HAY UN AMPLIO LISTADO DE CLÁUSULAS NULAS

EN GENERAL SON ABUSIVAS

Según la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios

Artículo Décimo bis.

1. Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente y todas aquéllas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato. En todo caso, se considerarán cláusulas abusivas los supuestos de estipulaciones que se relacionan en la disposición adicional primera de esta Ley.

Entre las muchas cláusulas abusivas de la Disposición adicional:

2. La reserva a favor del profesional de facultades de interpretación o modificación unilateral del contrato sin motivos válidos especificados en el mismo, así como la de resolver anticipadamente un contrato con plazo determinado si al consumidor no se le reconoce la misma facultad o la de resolver en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable un contrato por tiempo indefinido, salvo por incumplimiento del contrato o por motivos graves que alteren las circunstancias que motivaron la celebración del mismo.

4. La supeditación a una condición cuya realización dependa únicamente de la voluntad del profesional para el cumplimiento de las prestaciones, cuando al consumidor se le haya exigido un compromiso firme.

5. La consignación de fechas de entrega meramente indicativas condicionadas a la voluntad del profesional.

14. La imposición de renuncias o limitación de los derechos del consumidor.

15. La imposición de obligaciones al consumidor para el cumplimiento de todos sus deberes y contraprestaciones, aun cuando el profesional no hubiere cumplido los suyos.

26. La sumisión a arbitrajes distintos del de consumo, salvo que se trate de órganos de arbitraje institucionales creados por normas legales para un sector o un supuesto específico.

27. La previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si fuera inmueble, así como los de renuncia o transacción respecto al derecho del consumidor a la elección de fedatario competente según la Ley para autorizar el documento público en que inicial o ulteriormente haya de formalizarse el contrato.

28. La sumisión del contrato a un Derecho extranjero con respecto al lugar donde el consumidor emita su declaración negocial o donde el profesional desarrolle la actividad dirigida a la promoción de contratos de igual o similar naturaleza.

Artículo 10. Efectos.

1. La no incorporación al contrato de las cláusulas de las condiciones generales o la declaración de nulidad de las mismas no determinará la ineficacia total del contrato,

si éste puede subsistir sin tales cláusulas, extremo sobre el que deberá pronunciarse la sentencia.

2. La parte del contrato afectada por la no incorporación o por la nulidad se integrará con arreglo a lo dispuesto por el artículo 1258 del Código Civil y disposiciones en materia de interpretación contenidas en el mismo.

8. Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista. información en venta a distancia. no necesario registro

CAPÍTULO II.

VENTAS A DISTANCIA.

Artículo 38. Concepto.

1. Se consideran ventas a distancia las celebradas sin la presencia física simultánea del comprador y del vendedor, siempre que su oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia y dentro de un sistema de contratación a distancia organizado por el vendedor.

2. Las empresas de ventas a distancia que difundan sus ofertas por medios que abarquen el territorio de más de una Comunidad Autónoma se inscribirán en el Registro especial que a tal efecto funcione en el Ministerio de Economía, que recogerá los datos suministrados por las Comunidades Autónomas donde cada empresa tenga su domicilio social, coincidentes con los que figuren en el respectivo Registro autonómico, cuando haya sido establecido de acuerdo con lo previsto en el anterior artículo 37.

Las empresas no establecidas en España que practiquen ventas a distancia en territorio español se inscribirán directamente, a efectos informativos, en el Registro del Ministerio de Economía.

El Ministerio de Economía informará a las Comunidades Autónomas de las empresas de venta a distancia registradas.

Del mismo modo, las Comunidades Autónomas comunicarán a la Administración General del Estado las modificaciones que se produzcan en el registro autonómico correspondiente.

3. La regulación establecida en la presente Ley para las ventas a distancia no será de aplicación a:

Las ventas celebradas mediante distribuidores automáticos o locales comerciales automatizados.

Las ventas celebradas en subastas, excepto las efectuadas por vía electrónica.

4. Los artículos 39.1, 40, 43.1, 44 y 47 no serán de aplicación a los contratos de suministro de productos alimenticios, de bebidas o de otros bienes del hogar de consumo corriente suministrados en el domicilio del consumidor, en su residencia o en su lugar de trabajo por distribuidores que realicen visitas frecuentes y regulares.

5. El apartado 2 anterior y el artículo 37 no se aplicarán a las actividades de prestación de servicios de la sociedad de la información y comercio electrónico.

6. Cuando la contratación a distancia de bienes o servicios se lleve a cabo a través de medios electrónicos, se aplicará preferentemente la normativa específica sobre servicios de la sociedad de la información y comercio electrónico.

7. Las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica equivalentes se regirán por su normativa específica.

8. La validez y eficacia de los contratos relativos a bienes inmuebles quedará condicionada al cumplimiento de los requisitos que impone su legislación específica.

Regulación específica del Registro

Real Decreto 225/2006, de 24 de febrero, por el que se regulan determinados aspectos de las ventas a distancia y la inscripción en el registro de empresas de ventas a distancia.

Visita

http://www.mcx.es/VentaDistancia/principal.asp

TENGA EN CUENTA LO QUE AFIRMA LA EXPOSICIÓN DE ESTE REAL DECRETO:
Por otro lado, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, ha venido a introducir una regulación específica para las actividades de comercio electrónico, estableciendo unos requisitos de información para los prestadores de estos servicios. **Por este motivo, ya no resulta necesaria la obligación de registrar su actividad en el Registro de empresas de venta a distancia, cuando una empresa utilizando los servicios de operadores de telecomunicaciones, portales, o cualquier otro servicio de acceso a Internet, ofrezca y venda sus productos a través de este medio**, toda vez que la Ley de Servicios de la Sociedad de la Información ya contiene los elementos de la identificación de la empresa oferente adecuados al propio canal de comunicación a distancia, en este caso Internet y correo electrónico. No obstante, las obligaciones del contrato de compraventa surgidas por este medio, se regirán sustancialmente por lo dispuesto en el Capítulo II del Titulo III de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista en materia de contratos de venta a distancia. Igualmente, cabría precisar que si bien las empresas que utilicen los servicios de la sociedad de la información como canal de ventas no están obligadas a inscribirse en el Registro de empresas de venta a distancia, sí están obligadas a registrarse aquellas empresas que además de este canal utilizan otros medios como el catálogo, el teléfono, etc.

(extractos)

Artículo 2. Definición del Registro.

El Registro de empresas de ventas a distancia se configura como un órgano de carácter público y naturaleza administrativa, dependiente de la Dirección General de Política Comercial del Ministerio de Industria, Turismo y Comercio, cuyo objetivo es la obtención de información de las empresas que practican la modalidad de ventas a distancia en el territorio español, así como la elaboración de un censo actualizado de las mismas.

Artículo 5. Ámbito de aplicación. (FÍJESE QUE NO MENCIONA INTERNET)

1. Deberán inscribirse en el Registro de empresas de ventas a distancia, las empresas de comercio minorista que tengan dispuesto un sistema de contratación a distancia a través de las siguientes técnicas de comunicación a distancia:

Catálogo.

Impreso sin o con destinatario.

Carta normalizada.

Publicidad en prensa con cupón de pedido.

Teléfono.

Radio.

Televisión.

Visiófono (teléfono con imagen).

Vídeo texto.

Fax (telecopia).

2. Se exceptúan del ámbito de aplicación de este Real Decreto, sin perjuicio de las obligaciones de autorización e inscripción que, en su caso, establezcan las normas autonómicas de acuerdo con el marco legal vigente, las siguientes empresas:

Las empresas que desarrollando su actividad comercial en establecimiento fijo, esporádicamente pudieran realizar ventas a distancia, si el monto de las mismas en ningún caso constituye valor significativo de venta, ni constituye actividad ordinaria.

Las empresas de servicios de la sociedad de información.

Las empresas que realicen la prestación de servicios financieros ya sea en el ámbito de los mercados de valores, instituciones de inversión colectiva o en el ámbito bancario o asegurador.

Las empresas de venta de medicamentos, de acuerdo con la Ley 25/1990, de 20 de diciembre, del Medicamento.

.

(Ley comercio minorista, continúa…)

Artículo 40. Información previa.

1. Antes de iniciar el procedimiento de contratación y con la antelación necesaria, el vendedor deberá suministrar al consumidor, de forma veraz, eficaz y suficiente, la siguiente información:

La identidad del vendedor y su dirección.

Las características esenciales del producto.

El precio, incluidos todos los impuestos.

Los gastos de entrega y transporte, en su caso.

La forma de pago y modalidades de entrega o de ejecución.

La existencia de un derecho de desistimiento o resolución, o su ausencia en los contratos a que se refiere el artículo 45.

El coste de la utilización de la técnica de comunicación a distancia cuando se calcule sobre una base distinta de la tarifa básica.

El plazo de validez de la oferta y del precio.

La duración mínima del contrato, si procede, cuando se trate de contratos de suministro de productos destinados a su ejecución permanente o repetida.

Las circunstancias y condiciones en que el vendedor podría suministrar un producto de calidad y precio equivalentes, en sustitución del solicitado por el consumidor, cuando se quiera prever esta posibilidad.

En su caso, indicación de si el vendedor dispone o está adherido a algún procedimiento extrajudicial de solución de conflictos.

2. La información contenida en el apartado anterior, cuya finalidad comercial debe ser indudable, deberá facilitarse al comprador de modo claro, comprensible e inequívoco, mediante cualquier técnica adecuada al medio de comunicación a distancia utilizado, y deberá respetar, en particular, el principio de buena fe en las transacciones comerciales, así como los principios de protección de quienes sean incapaces de contratar.

9. Garantías contratación a distancia en Ley comercio minorista: consentimiento, desestimiento, pago con tarjeta

Artículo 41. Necesidad de consentimiento expreso.

1. En ningún caso la falta de respuesta a la oferta de venta a distancia podrá considerarse como aceptación de ésta.

2. Si el vendedor, sin aceptación explícita del destinatario de la oferta, enviase a éste el producto ofertado, se aplicará lo dispuesto en el artículo siguiente.

Artículo 42. Prohibición de envíos no solicitados.

Queda prohibido enviar al consumidor artículos o mercancías no pedidos por él al comerciante cuando dichos suministros incluyan una petición de pago. En caso de que así se haga, y sin perjuicio de la infracción que ello suponga, el receptor de tales artículos no estará obligado a su devolución, ni podrá reclamársele el precio.

En caso de que decida devolverlo no deberá indemnizar por los daños o deméritos sufridos por el producto.

No será de aplicación lo dispuesto en el párrafo primero cuando quede claramente de manifiesto al receptor que el envío no solicitado se debía a un error, correspondiendo al vendedor la carga de la prueba. El receptor tendrá derecho a ser indemnizado por los gastos y por los daños y perjuicios que se le hubieran causado.

Artículo 43. Ejecución y pago.

1. Salvo que las partes hayan acordado otra cosa, el vendedor deberá ejecutar el pedido a más tardar en el plazo de treinta días a partir del día siguiente a aquel en que el comprador le haya comunicado su pedido.

2. En caso de no ejecución del contrato por parte del vendedor por no encontrarse disponible el bien objeto del pedido, el comprador deberá ser informado de esta falta de disponibilidad y deberá poder recuperar cuanto antes, y en cualquier caso en un plazo de treinta días como máximo, las sumas que haya abonado. En el supuesto de que el vendedor no realice este abono en el plazo señalado, el comprador podrá reclamar que se le pague el doble de la suma adeudada, sin perjuicio a su derecho de ser indemnizado por los daños y perjuicios sufridos en lo que excedan de dicha cantidad.

3. De no hallarse disponible el bien objeto del pedido, cuando el consumidor hubiera sido informado expresamente de tal posibilidad, el vendedor podrá suministrar sin aumento de precio un producto de características similares que tenga la misma o superior calidad. En este caso, el comprador podrá ejercer sus derechos de desistimiento y resolución en los mismos términos que si se tratara del bien inicialmente requerido.

Artículo 44. Derecho de desistimiento.

1. El comprador dispondrá de un plazo mínimo de siete días hábiles para desistir del contrato sin penalización alguna y sin indicación de los motivos. Será la ley del lugar donde se ha entregado el bien la que determine qué días han de tenerse por hábiles.

2. El ejercicio del derecho de desistimiento no estará sujeto a formalidad alguna, bastando que se acredite en cualquier forma admitida en derecho.

3. El derecho de desistimiento no puede implicar la imposición de penalidad alguna, si bien podrá exigirse al comprador que se haga cargo del coste directo de devolución del producto al vendedor.

No obstante lo anterior, en los supuestos en que el vendedor pueda suministrar un producto de calidad y precio equivalentes, en sustitución del solicitado por el consumidor, los costes directos de devolución, si se ejerce el derecho de desistimiento, serán por cuenta del vendedor que habrá debido informar de ello al consumidor.

Serán nulas de pleno derecho las cláusulas que impongan al consumidor una penalización por el ejercicio de su derecho de desistimiento o la renuncia al mismo.

4. A efectos del ejercicio del derecho de desistimiento, el plazo se calculará a partir del día de recepción del bien, siempre que se haya cumplido el deber de información que impone el artículo 47.

5. En el caso de que el vendedor no haya cumplido con tal deber de información, el comprador podrá resolver el contrato en el plazo de tres meses a contar desde aquel en que se entregó el bien. Si la información a que se refiere el artículo 47 se facilita durante el citado plazo de tres meses, el período de siete días hábiles para el desistimiento empezará a correr desde ese momento. Cuando el comprador ejerza su derecho a resolver el contrato por incumplimiento del deber de información que incumbe al vendedor, no podrá éste exigir que aquel se haga cargo de los gastos de devolución del producto.

6. Cuando el comprador haya ejercido el derecho de desistimiento o el de resolución conforme a lo establecido en el presente artículo, el vendedor estará obligado a devolver las sumas abonadas por el comprador sin retención de gastos. La devolución de estas sumas deberá efectuarse lo antes posible y, en cualquier caso, en un plazo máximo de treinta días desde el desistimiento o la resolución. Corresponde al vendedor la carga de la prueba sobre el cumplimiento del plazo. Transcurrido el mismo sin que el comprador haya recuperado la suma adeudada, tendrá derecho a reclamarla duplicada, sin perjuicio de que además se le indemnicen los daños y perjuicios que se le hayan causado en lo que excedan de dicha cantidad.

7. En caso de que el precio haya sido total o parcialmente financiado mediante un crédito concedido al comprador por parte del vendedor o por parte de un tercero previo acuerdo de éste con el vendedor, el ejercicio del derecho de desistimiento o de resolución contemplados en este artículo implicará al tiempo la resolución del crédito sin penalización alguna para el comprador.

8. El transcurso del plazo del derecho de desistimiento sin ejecutarlo no será obstáculo para el posterior ejercicio de las acciones de nulidad o resolución del contrato cuando procedan conforme a derecho.

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

Artículo 5. Atribución de la carga de la prueba.

1. La carga de la prueba sobre la existencia y contenido de la información previa de las cláusulas del contrato; de la entrega de las condiciones generales; de la justificación documental de la contratación una vez efectuada; de la renuncia expresa al derecho de resolución; así como de la correspondencia entre la información, entrega y justificación documental y el momento de sus respectivos envíos, corresponde al predisponente.

2. A estos efectos, y sin perjuicio de cualquier otro medio de prueba admitido en derecho, cualquier documento que contenga la citada información aun cuando no se haya extendido en soporte papel, como las cintas de grabaciones sonoras, los disquetes y, en particular, los documentos electrónicos y telemáticos, siempre que quede

garantizada su autenticidad, la identificación fiable de los manifestantes, su integridad, la no alteración del contenido de lo manifestado, así como el momento de su emisión y recepción, será aceptada en su caso, como medio de prueba en los términos resultantes de la legislación aplicable.

Para ello, en los casos de contratación electrónica, deberá utilizarse una firma electrónica avanzada que atribuya a los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita, conforme a lo dispuesto en el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica. En estos casos, al documento electrónico se acompañará una consignación de fecha y hora de remisión y recepción, en su caso.

(continúa ley comercio minorista…)

Artículo 45. Excepciones al derecho de desistimiento.

Salvo pacto en contrario, lo dispuesto en el artículo anterior no será aplicable a los siguientes contratos:

Contratos de suministro de bienes cuyo precio esté sujeto a fluctuaciones de coeficientes del mercado financiero que el vendedor no pueda controlar.

Contratos de suministro de bienes confeccionados conforme a las especificaciones del consumidor o claramente personalizados, o que, por su naturaleza, no puedan ser devueltos o puedan deteriorarse o caducar con rapidez.

Contratos de suministro de grabaciones sonoras o de vídeo, de discos y de programas informáticos que hubiesen sido desprecintados por el consumidor, así como de ficheros informáticos, suministrados por vía electrónica, susceptibles de ser descargados o reproducidos con carácter inmediato para su uso permanente.

Contratos de suministro de prensa diaria, publicaciones periódicas y revistas.

Artículo 46. Pago mediante tarjeta.

1. 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.

2. Sin embargo, si la compra hubiese sido efectivamente realizada por el titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución reconocido en el artículo 44 y, por tanto, hubiese exigido indebidamente la anulación del correspondiente cargo, aquel quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación.

Artículo 47. Información. (ver información)

10. Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores

Basta recordar su existencia y regulación particular.

CAPÍTULO I. OBJETO, ÁMBITO DE APLICACIÓN Y CARÁCTER IMPERATIVO DE LOS DERECHOS RECOGIDOS EN LA LEY.

Artículo 1. Objeto.

Artículo 2. Ámbito subjetivo de aplicación.

Artículo 3. Carácter imperativo.

Artículo 4. Ámbito material.

CAPÍTULO II. RÉGIMEN DE LOS CONTRATOS A DISTANCIA.

Artículo 5. Las partes.

Artículo 6. Instrumentos técnicos.

Artículo 7. Requisitos de información previa al contrato.

Artículo 8. Requisitos adicionales de información.

Artículo 9. Comunicación de las condiciones contractuales y de la información previa.

Artículo 10. Derecho de desistimiento.

Artículo 11. Pago del servicio prestado antes del desistimiento.

Artículo 12. Pago mediante tarjeta.

Artículo 13. Servicios no solicitados.

Artículo 14. Comunicaciones no solicitadas.

Artículo 15. Acciones de cesación.

Artículo 16. Reclamación extrajudicial.

Artículo 17. Carga de la prueba.

CAPÍTULO III. RÉGIMEN SANCIONADOR.

Artículo 18. Sanciones administrativas.

DISPOSICIÓN ADICIONAL PRIMERA. Modificación de la Ley 26/1984, 19 de julio, general para la defensa de consumidores y usuarios.

DISPOSICIÓN ADICIONAL SEGUNDA. Plan de medidas de lucha contra las actividades de captación a distancia de información confidencial de forma fraudulenta.

DISPOSICIÓN DEROGATORIA.

DISPOSICIÓN FINAL PRIMERA. Competencia constitucional.

DISPOSICIÓN FINAL SEGUNDA. Incorporación de Derecho de la Unión Europea.

DISPOSICIÓN FINAL TERCERA. Entrada en vigor.

CAPÍTULO I.

OBJETO, ÁMBITO DE APLICACIÓN Y CARÁCTER IMPERATIVO DE LOS DERECHOS RECOGIDOS EN LA LEY.

Artículo 1. Objeto.

Esta Ley establece el régimen específico que habrá de aplicarse a los contratos con consumidores de servicios financieros prestados, negociados y celebrados a distancia, sin perjuicio de la aplicación de la normativa general sobre servicios de la sociedad de la información y comercio electrónico que se contiene en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico y, en su caso, en el capítulo II del Título III y disposición adicional primera de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista y demás normativa de aplicación general a los consumidores, así como la normativa especial que rige la prestación de los servicios financieros en cada caso.

Artículo 4. Ámbito material.

1. Se comprenden en el ámbito de la Ley los contratos celebrados entre un proveedor y un consumidor y las ofertas relativas a los mismos siempre que generen obligaciones para el consumidor, cuyo objeto es la prestación de todo tipo de servicios financieros a los consumidores, en el marco de un sistema de venta o prestación de servicios a distancia organizado por el proveedor, cuando utilice exclusivamente técnicas de comunicación a distancia, incluida la propia celebración del contrato.

…

2. A los efectos de la presente Ley, se entenderán por servicios financieros los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros….

3. Se entiende que el contrato se celebra a distancia cuando para su negociación y celebración se utiliza exclusivamente una técnica de comunicación a distancia, sin presencia física y simultánea del proveedor y el consumidor, consistente en la utilización de medios telemáticos, electrónicos, telefónicos, fax u otros similares.

11. Descripcion del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.

Sumario:

DISPOSICIÓN TRANSITORIA PRIMERA. Vigencia de normas.

DISPOSICIÓN TRANSITORIA SEGUNDA. Especificaciones de la portabilidad.

DISPOSICIÓN TRANSITORIA TERCERA. Códigos para la prestación de servicios de tarificación adicional.

DISPOSICIÓN DEROGATORIA ÚNICA. Derogación normativa.

DISPOSICIÓN FINAL PRIMERA. Modificación del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre.

DISPOSICIÓN FINAL SEGUNDA. Título competencial.

DISPOSICIÓN FINAL TERCERA. Incorporación de derecho de la Unión Europea.

DISPOSICIÓN FINAL CUARTA. Facultades de desarrollo.

DISPOSICIÓN FINAL QUINTA. Entrada en vigor.

Cuestionario sobre Contratación y consumo electrónicos

Tenga en cuenta quién está establecido en España según artículo 2 y 3 de la LSSICE

Jurisdicción y ley aplicable

Jurisdicción aplicable, regla general de la Ley orgánica poder judicial.
Si no es contratación de consumo, es posible pactar qué jurisdicción y qué juzgados serán los competentes? Si no se ha pactado nada, si el contratante demandado está en España, qué juzgado es competente? (art. 22. 2).
En materia de contratación de consumo, qué regla general observas del artículo 22. 4º, que el consumidor tiene que ir al país del vendedor a demandarle, o siempre podrá hacerlo en su país? Si la página web extranjera no dice nada de que oferta sus productos para España, pero he comprado porque me interesaba el precio, en principio podrás demandarle en España.

Ley aplicable general en Código civil
Según el artículo 10 del Código Civil y como regla general.
Señale por el orden aplicable qué ley se aplica en el ámbito de contratos, piense su aplicabilidad a internet. Tenga en cuenta la importancia que tendrá el lugar de la celebración del contrato.

Para el ámbito económico europeo regido por el Convenio de Roma (versión 2008):
¿La ley aplicable en general es la del consumidor, o la del profesional?
¿El "profesional" que ponga en la web la posibilidad de contratar de forma abierta a cualquier usuario de internet, crees que se somete a la ley del consumidor?
Bajo qué presupuesto puede el "profesional" eludir la aplicación de la ley del consumidor?
¿Se aplica lo anterior a un billete de avión? ¿Y si es un billete de avión vinculado a un paquete turístico contratado con una agencia de viajes?
¿Y si he contratado la compra de un inmueble a través de internet, se aplica lo anterior?
(Art. 6)
Aunque en general la ley aplicable es la del consumidor ¿Es posible pactar la ley aplicable?

¿Aunque se pacte la ley aplicable para el vendedor, por ejemplo, es posible aplicar las garantías que tenga el consumidor en su país?

Según art. 3. 1º d) se aplica la LSSICE para obligaciones de contratos de consumo?

Regulación general contratación electrónica LSSICE

Los contratos electrónicos, ¿se rigen sólo por la LSSICE? ¿Qué normas más rigen estos contratos? (ver art. 23 LSSICE y tenga en cuenta otras normas citadas en material).

¿Qué contratos se rigen por su legislación específica?

No olvide las obligaciones de información previa (información general art. 10 Lssice, ART. 27 LSSICE)

¿Cuándo se considera celebrado un contrato celebrado electrónicamente? (Ver disposición adicional 4ª, y la redacción de los artículos 1262 Código civil/ 54 C. Comercio)

-Juan me ofrece la venta del coche por medios electrónicos, por un precio de 1000 euros, el viernes le mando un correo electrónico para decirle que acepto, pero él está de viaje. Cuando vuelve, ese fin de semana un vecino le dice a Juan que le compra el coche, Juan llega al trabajo y ve mi correo, dice que no tiene ninguna obligación..

¿Al haber aceptado la oferta el viernes, según puedo demostrar con mi correo electrónico, puede decirse que el contrato ya estaba vigente, por lo que Juan no puede incumplir el contrato?

Y si Juan ve el correo electrónico mío el lunes, pero pese a mi solicitud no me contesta, si bien, mi gestor de correo me da un aviso de que sí ha leído el correo. Sin embargo no sé nada de Juan pese a mi insistencia en que sí quiero el coche por 1000 euros. Al final, el miércoles le llamo por teléfono y me dice que se lo acaba de vender al vecino por 1200. ¿Era ya vigente mi contrato, por lo que lo ha incumplido?

En principio, en virtud del artículo 28, ¿Juan estaba obligado a decirme que sabía que le había dicho que sí a su oferta del coche?

El comprador en mi web ha aceptado todos los términos y ya ha comprado, qué es obligatorio que yo haga (o que automatizadamente haga la aplicación o sistema informático que yo utilice para la gestión de las compraventas de mi web).

Lugar del contrato

Donde se presume celebrado el contrato en general? (art. 1256 CC).

Donde se presume celebrado el contrato en los que sea parte un consumidor (art. 29).

Donde se presume celebrado el contrato entre empresarios o profesionales.

Crees que es posible pactar que se considere celebrado el contrato en otro lugar?

LMISI 2007: nueva obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.

¿Qué concepto se ha utilizado par señalar quiénes son los obligados por este artículo 2?

A la vista de los requisitos que se fijan para determinar qué empresas son, señala 5 empresas obligadas de los distintos tipos que se enuncian:

1.
2.
3.
4.
5.

¿Qué cuatro trámites son los obligados a través de internet para estas empresas:

1.

2.

3.

4.

Información obligatoria contratación electrónica y de consumidores

(recuerde en todo caso el artículo 10 LSSICE)

Información LSSICE (no art. 10).

-Comercializo los productos de mi empresa destinados a los consumidores a través de internet, dispongo de una web para ello, ¿tengo que dar alguna información previa antes de que se proceda a la contratación? ¿cuál?

He ofertado uno de mis productos en la web a un precio de 25 euros. ¿Hasta cuándo se considera válida dicha oferta y por tanto, me obliga?

Soy empresario y contrato con otro empresario habitualmente por medios electrónicos, ¿hemos de sujetarnos a la información previa y posterior de los artículos 27 y 28?

En la web han dejado la oferta de una impresora muy bien de precio. Me dicen que es de una oferta del año pasado, pero no hay nada que así lo indique. En razón del artículo 27. 3º sigue siendo vinculante esa oferta?

Por cuanto a la obligación de facilitar un ejemplar de las condiciones generales de contratación en la Ley 7/1998, tenga en cuenta el artículo 2 del Real Decreto 1906/1999. Piense en la contratación a través de internet, de una página web, cómo considera que puede cumplirse la obligación que se impone?

Y si se trata de la contratación de un servicio a través del teléfono móvil, cómo cree que se cumpliría la obligación, podría valer con la remisión a una web donde sean accesibles tales condiciones?

Información en Ley 7/1996

Siga las obligaciones de información del artículo 40 y del artículo 47.

INFORMACIÓN:

Si la venta a distancia más allá de una Comunidad Autónoma está sujeta a autorización, hay obligación de información sobre los datos de la autorización obtenida en la página web? Lea el artículo 10 de la LSSICE al respecto.

Cómo debe aparecer en la página web la información del artículo 40, según el artículo 40. 2º Ley comercio minorista

Compro las zapatillas por internet. Señale sintéticamente qué información he de recibir al momento que haya culminado la operación según el art. 47. Ley comercio minorista

sEgún el artículo 47. 2º Ley comercio minorista cómo crees que es posible que se me facilite la información al momento de culminar mi compra por internet.

Actividad general sobre deberes de información

ACTIVIDAD GENERAL SOBRE DEBERES DE INFORMACIÓN

Simule que tiene que poner el texto de una página web legal que vende para toda España unas zapatillas deportivas y ponga toda la información del artículo 10 LSSICE, así como todos los requisitos de información previa del artículo 27 de la LSSICE y del artículo 40 de la Ley de comercio minorista. Tenga en cuenta el artículo 47 de la ley.

Tenga en cuenta las obligaciones de información sobre condiciones generales de contratación.

Extienda la simulación a todas las obligaciones de información en la ejecución del contrato o posterior al consentimiento (art. 28 LSSICE y art. 47 Ley comercio minorista).

NOTA: simule e invente datos, no pierda tiempo en hacerlo: ejemplo: condiciones generales de la contratación: 1º xxxx, 2º yyyy y 3º wwww.
Ejemplo: Nombre de la empresa xxxx, lugar yyyy, etc.

Ley 7/1998, sobre condiciones generales de la contratación

Según el artículo 1. 1º qué son las condiciones generales de la contratación. Se te ocurre un ejemplo donde las veas habitualmente.

Según el artículo 5, cuándo pasan a formar parte del contrato las condiciones generales.

Según el artículo 5. 3, cómo se consideran las cláusulas del contrato? Es necesaria la firma escrita? Observa el requisito específico de "enviar inmediatamente justificación escrita de la contratación efectuada. Se te ocurre cómo se puede cumplir este requisito en la e-contratación?

Señala cuáles son las reglas básicas de interpretación de las condiciones generales y a quién deben beneficiar las dudas (Art. 6).

Observa según el artículo 7 las condiciones que se entienden "no incorporadas", vincúlalas con la información real del artículo 5. 3º.

Según el artículo 8 son nulas las condiciones generales abusivas.

Cuál es la definición general de cláusula abusiva (art. 10 bis. 1º Ley 26/1984)

Entre las muchas cláusulas abusivas. Es posible que quede en manos del vendedor resolver el contrato a su juicio, con qué condiciones? (nº 2)

Crees que un prestador de servicios de intermediación, por ejemplo, un alojador de contenidos puede considerar que los contenidos "cargados" por el cliente –que incluso aloja gratuitamente- son contrarios a sus condiciones generales y, por ello, sin aviso previo, retirar tales contenidos? Sobre qué base consideras tu respuesta?

Si ofreces venta de productos por internet puedes decir que las fechas de entrega son meramente indicativas?

Puede haber una condición general que suponga que el consumidor renuncia a un derecho? Sobre qué base consideras tu respuesta?

Crees que para contratar con consumidores a distancia puede haber una condición general que someta a un arbitraje que no sea de consumo? (indica la base de tu respuesta)

Crees que para contratar con consumidores a través de internet una cláusula puede decir que si hay conflicto se resolverá la cuestión en los tribunales del lugar del vendedor? Si lo dice y tu lo aceptas, qué sucede? (indica la base de tu respuesta)

Compro una cámara de fotos en una web canadiense que vende en castellano y con indicativo de banderita española. En las condiciones dice que se me aplicará el Derecho canadiense. Si lo dice y tu lo aceptas, qué sucede? (indica la base de tu respuesta)

Según el artículo 10, si hay condiciones generales nulas o que se tengan por no puestas, ¿la contratación es nula?, qué sucede. (indica la base de tu respuesta)

Cuestiones generales de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista

Según el artículo 38, crees que si vendes a través de internet debes inscribirte en un Registro especial? Lee en especial el apartado 2 y el apartado 5. Crees que un "simple" prestador de servicios de la sociedad de la información que no realiza ventas a distancia, debe inscribirse en tal registro? Tenga en cuenta que la LSSICE no exige autorización previa general.

Sigue la regulación del registro, Real Decreto 225/2006, de 24 de febrero, por el que se regulan determinados aspectos de las ventas a distancia y la inscripción en el registro de empresas de ventas a distancia.

¿De quién depende el Registro? ¿Qué finalidad tiene? Si comercializas u ofreces servicios a través de internet, ¿es necesario estar registrado y autorizado?

Información y garantías en Ley comercio minorista

Recibe un mail que le indica que si no dice nada, se tendrá por aceptada la oferta de unas bonitas zapatillas. Ud. no contesta. Días después recibe el

producto pidiéndole el pago. Ante lo bonito de las zapatillas, decide usarlas. ¿Tiene UD. que pagarlas? (Arts. 41 y 42.

Según el artículo 43 y salvo otro pacto, en qué plazo debe librarse el pedido de un producto por internet?

Compré las zapatillas en la página web, pero se han acabado. Tengo derecho a que me devuelvan el dinero, en qué plazo? Es posible que me propongan el envío de unas zapatillas similares? Puedo negarme? (art. 43 y 44).

Derecho de desistimiento art. 44.

He comprado unas zapatillas por internet. He visitado luego otra página web y las veo más baratas. Puedo conseguir comprarlo en la otra página web sin tener que culminar mi compra de las zapatillas?

Qué plazo tengo para desistir de lo que he contratado en internet? Cómo se miden los días hábiles? Desde cuándo (art. 44. 1 y 4º)

Me puede costar algún dinero desistir de un contrato por internet en el plazo correspondiente?

El vendedor no dispuso la información del artículo 47 de la ley. He comprado mis zapatillas, las recibí y un mes y medio después. No las he usado. Puedo resolver el contrato según el artículo 44. ¿Quién debe cargar con los gastos de envío del producto del contrato resuelto?

Real Decreto 1906/1999

Según el artículo 5, a quién correspondería probar que sí que se cumplieron los diversos requisitos de información cuyo incumplimiento puede generar los derechos de resolución o desistimiento?

(continúa ley…)

Ya haya resuelto el contrato, o desistido, qué plazo tiene el vendedor para devolverme el total del precio pagado? Puede retenerme los gastos de envío de las zapatillas? Ha pasado un mes y no me devuelven el dinero? Qué derecho tengo?

En vez de unas zapatillas, compré un equipo de música a través de un crédito que me ofreció el mismo vendedor por internet. He desistido o resuelto el contrato. Qué sucede con ese crédito. Me puede costar algún dinero?

Puedo ejercer el derecho a desistir cuando las zapatillas me las confeccionaron para mí sobre la base del dibujo personalizado de mi pié (art. 45?

Puedo ejercer el derecho a desistir de la compra de unos yogures en el Mercadona?

Puedo ejercer el derecho a desistir de la compra de unos CDS de música o de las canciones compradas a través de internet?

Tarjeta de crédito (art. 46).

Me han cargado la compra de unas zapatillas en mi cuenta. No tengo idea del origen de ese cargo. Puedo exigir que anulen mi cargo?

Compré las zapatillas, como no me gustan solicito a mi entidad que anule el cargo según el artículo 46. Si obtengo la anulación, quién correrá con los daños que cause al vendedor de las zapatillas?

VII. CONTROL Y SANCIONES ADMINISTRATIVAS DE LA LSSICE

1. Cuento de la LSSICE y régimen disciplinario

Adaptado de Javier A. Maestre maestre@dominiuris.com Abogado.

Nota: Texto actualizado a la redacción final de la Ley.

Un día un hombre con gabardina le preguntará:

- Oiga, usted tiene página Web ¿no? Bien, me enseña el certificado de inscripción del nombre de dominio o dirección de Internet que usa en el registro donde se encuentra inscrito para fines de publicidad o para adquirir su personalidad jurídica.

- Nuestra dirección es "tienda.tañabueyes.com" y, que yo sepa, no lo tenemos notificado a ningún sitio.

- Falta de notificación del dominio o dirección de Internet para la realización de una actividad económica, infracción leve art. 38.4.a) LSSICE. Bien,

¿Qué información suministra en la Web sobre su establecimiento?

- El correo electrónico nada más, todo el mundo sabe dónde estamos

-Incumplimiento de lo establecido en las letras a) y f) del artículo 10.1. Infracción grave, art. 38.3.a) LSSICE. Bien,

¿En qué Condiciones efectúa usted las comunicaciones comerciales?

-Bueno, cuando me llega una novedad de la capital, mando un correillo a los que puedan estar interesados.

-Vaya, incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

Infracción leve, art. 38.4.c). Denuncia a la Agencia de Protección de datos. ¿Han prestado esas personas su consentimiento para la remisión de los mensajes? ¿Cuántos mensajes les ha remitido en el último año?

-Hombre, como tal, no lo he hecho, pero nunca se han quejado. En el último año les habré enviado unos 4 o 5 mensajes

-El envío, en el plazo de un año, de más de 3 comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan autorizado su remisión. Infracción grave, art. 38.3.b). ¿Realiza Ud. transacciones o contratos a través de la Red?

-Bueno, la Mariana, no sale de casa, me hace el pedido por Internet y luego por la tarde el chico le lleva la compra.

-No proporcionar al destinatario del servicio, por medios electrónicos, las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el

artículo 27. Infracción grave art. 38.3.c). ¿Confirma usted la aceptación de la compra o ha pactado su exclusión en el contrato con el consumidor?

-Yo pongo en el pedido lo que ella me pide en el correo, pero nunca ha habido ningún problema.

-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, infracción grave, art. 38.3.d).Me parece que por hoy ya está bien, ya volveré otro día para hacer una inspección más a fondo, de conformidad con lo establecido en el artículo 35 de la LSSICE. Sepa usted que, conforme a este precepto, tengo la consideración de autoridad pública, igual que un Inspector de Hacienda. Debe usted tener cuidado con su negocio, parece mentira que sea prestador de Servicios de la Sociedad de la Información: 2 infracciones leves, sanción máxima de 30.000 Euros por cada una. Total 60.000 Euros. 4 infracciones graves, sanción máxima de 150.000 Euros por cada una. Total 600.000 Euros. En total 660.000 Euros o 109.814.760 pesetas de las del año 2001.

2. Supervisión y control de la LSSICE

…Artículo 35. Supervisión y control.

Versión LMISI 2007

Artículo 35. Supervisión y control.

1. El Ministerio de Industria, Turismo y Comercio en el ámbito de la Administración General del Estado, y los órganos que correspondan de las Comunidades Autónomas, controlarán, en sus respectivos ámbitos territoriales y competenciales, el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. En todo caso, y no obstante lo dispuesto en el apartado anterior, cuando las conductas realizadas por los prestadores de servicios de la sociedad de la información estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan.

Artículo 36. Deber de colaboración.

1. Los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología y a los demás órganos a que se refiere el artículo anterior toda la información y colaboración precisas para el ejercicio de sus funciones.

Igualmente, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

2. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, estatales o autonómicas, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VII

Infracciones y sanciones

Artículo 37. Responsables.

Los prestadores de servicios de la sociedad de la información estén sujetos al régimen sancionador establecido en este Título cuando la presente Ley les sea de aplicación.

Artículo 38. Infracciones. Modificados los apartados 2,3 y 4 por ley 59/2003, de 19 de diciembre.

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.

2. Son infracciones muy graves:

LAS TACHADAS, YA NO POR LMISI 2007 (respecto de sanciones por retención de datos de tráfico, téngase en cuenta la LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

~~a.El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.~~

b. El incumplimiento de 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.

~~c.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.~~

~~d. La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.~~

3. Son infracciones graves:

~~a.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, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.~~

b. El incumplimiento significativo de lo establecido en los párrafos a y f del artículo 10.1.

c. 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.

3. Son infracciones 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, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.

El incumplimiento significativo de lo establecido en los párrafos a y f del artículo 10.1.

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 en el artículo 21.

El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, 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 el artículo 27.

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 lo establecido en el apartado 3 del artículo 10.

El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

~~La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.~~

Nuevo: incumplimiento de lo previsto en el artículo 12 bis

No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b, c, d, e y g del mismo, o en los párrafos a y f cuando no constituya infracción grave.

El incumplimiento de lo previsto en el artículo 20 para 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 en el artículo 21 y no constituya infracción grave.

No facilitar la información a que se refiere el artículo 27.1, 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 en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave.

Artículo 39. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

Por la comisión de infracciones graves, multa de 30.001 hasta 1 50.000 euros.

Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el Boletín Oficial del Estado, o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración pública o en la página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, por el número de usuarios o de contratos afectados, y la gravedad del ilícito.

3. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

Artículo 40. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

La existencia de intencionalidad.

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

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

La naturaleza y cuantía de los perjuicios causados.

Los beneficios obtenidos por la infracción.

Volumen de facturación a que afecte la infracción cometida.

Artículo 41. Medidas de carácter provisional.

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

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

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y

familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Nuevo por LMISI 2007

Artículo 43. Competencia sancionadora.

1. La imposición de sanciones por incumplimiento de lo previsto en esta Ley corresponderá al órgano o autoridad que dictó la resolución incumplida o al que estén adscritos los inspectores. Asimismo las infracciones respecto a los derechos y garantías de los consumidores y usuarios serán sancionadas por el órgano correspondiente de las Comunidades Autónomas competentes en materia de consumo.

2. En la Administración General del Estado, la imposición de sanciones por el incumplimiento de lo previsto en esta Ley 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.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.
3. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de

las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses

Artículo 44. Concurrencia de infracciones y sanciones.

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. Prescripción.

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Cuestionario sobre Control de la LSSICE y régimen disciplinario

Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores

Tenga en cuenta la existencia de esta ley para profundizar en ella de resultarle de interés.

Para qué ámbito se aplica esta ley (Art. 1)

Si se trata del objeto de esta ley, ya no se aplica la LSSICE?

Si se trata del objeto de esta ley, ya no se aplica la Ley de comercio minorista?

Según el artículo 4, para qué contratos se aplica esta ley 22/2007?

Cuándo se entiende que hay un contrato a distancia (Art. 4)?

Tenga en cuenta la información obligatoria, los plazos del derecho de desistimiento, la situación ante pagos de tarjeta, etc., que no se trasponen.

Cuento de la LSSICE, Supervisión y control de la LSSICE":

Haz un breve comentario sobre el **"cuento" de la LSSICE y su régimen disciplinario** y la impresión personal que te merece (10 líneas).

Qué Ministerio, en teoría, controla el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas por la LSSICE?

Si vendo viagra por internet, crees que la competencia es sólo del Ministerio anteriormente referido? (art. 35. 3º)

Alojo contenidos, me notifican la resolución judicial de su ilicitud con obligación de bloquear el acceso al contenido que alojo. Incumplo dicha orden, qué tipo de infracción cometo?

El "incumplimiento significativo" del deber de información del artículo 10, en sus letras a y f, qué tipo de infracción es?

Qué tipo de infracción es cualquier otro incumplimiento del deber de información del artículo 10?

Qué tipo de sanción es el No poner a disposición del destinatario del servicio las condiciones generales?

Sanción mínima-máxima por infracción muy grave

Sanción mínima-máxima por infracción grave

Sanción mínima-máxima por infracción leve

Que tipos de medidas provisionales se pueden adoptar si así se considera (art. 41).

Si no se cumple la medida provisional acordada qué multa se puede imponer?

VIII. DELITOS INFORMÁTICOS

Reforma Código penal en 2010

Téngase en cuenta la muy posible reforma de algunos artículos en 2010. Al respecto, un comentario de la misma de Carlos Sánchez Almeida en
Los delitos de intrusismo y vandalismo informático en el proyecto de reforma del Código Penal español
La hora de los hackers
http://www.rebelion.org/noticia.php?id=104870

1. Ataques que se producen contra el derecho a la intimidad.

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

CÓDIGO PENAL
(L.O. 10/1995, de 23 de noviembre)
Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrá las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198.

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199.

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce años.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200.

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Artículo 201.

1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4.º del artículo 130.

2. Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.

Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 270.

« 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.

Artículo 271.

«Se impondrá la pena de prisión de uno a cuatro años, multa de 12 a 24 meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias:

- a) Que el beneficio obtenido posea especial trascendencia económica.
- b) Que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente o a la especial importancia de los perjuicios ocasionados.
- c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual.
- d) Que se utilice a menores de 18 años para cometer estos delitos.

Artículo 272.

1. La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios.

2. En el supuesto de sentencia condenatoria, el Juez o Tribunal podrá decretar la publicación de ésta, a costa del infractor, en un período oficial.

artículo 287

« 1.Para proceder por los delitos previstos en la sección 3.ª de este capítulo será necesaria denuncia de la persona agraviada o de sus representantes legales. Cuando aquella sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el ministerio fiscal."

2. No será precisa la denuncia exigida en el apartado anterior cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

Artículo 288.

En los supuestos previstos en los artículos anteriores se dispondrá la publicación de la sentencia en los periódicos oficiales y, si lo solicitara el perjudicado, el Juez o Tribunal podrá ordenar su reproducción total o parcial en cualquier otro medio informativo, a costa del condenado.

Además, el Juez o Tribunal, a la vista de las circunstancias del caso, podrá adoptar las medidas previstas en el artículo 129 del presente Código.

¿Es delito bajarse música por Internet?, de El País (opiniones breves y diversas de varios juristas) (recuerde: que no sea delito no quiere decir que sea legal, puede ser ilícito)

http://www.periodistadigital.com/object.php?o=34223

La explosión del gratis total en la Red

El Pais (31/10/04, 04.34 horas)

Canal Motor Periodistadigital.com El 1 de octubre entraba en vigor el nuevo Código Penal, que ha intentado reforzar la protección la propiedad intelectual. Sin embargo, a día de hoy, los juristas no se ponen de acuerdo cuando tienen que responder a la pregunta de si los miles de internautas españoles que se descargan obras protegidas están cometiendo o no un delito penal y, por tanto, pueden acabar en la cárcel. El País ha planteado a seis expertos en Derecho de las tecnologías de la información una pregunta muy simple: "¿Es delito descargarse música desde Internet". Éstas son sus opiniones.

JOSÉ MARÍA ANGUIANO / Garrigues

SÍ

"A mi juicio, siempre ha sido delito descargarse música por Internet. La reforma del 1 de octubre, en el ámbito digital, tiene su reflejo en la nueva redacción del 270.3, que amplía la protección que hasta la reforma sólo otorgaba a los programas de ordenador a otras creaciones intelectuales. De esta forma se penaliza la fabricación, distribución e incluso la posesión de medios tecnológicos que faciliten la supresión no autorizada o la neutralización de las medidas de protección. De esta forma, cualquiera que suba a la Red una obra protegida que previamente haya tenido que desproteger se le podrá aplicar este apartado del artículo 270".

JAVIER CREMADES / Cremades & Calvo Sotelo

NO

"Hay que precisar que en el derecho penal rige el principio de la tipicidad de la conducta supuestamente delictiva, esto es, que se encuentre expresamente consagrada

como delito en el Código Penal. El debate abierto en relación a este tema se debe a una interpretación equivocada de la modificación del artículo 270 del Código Penal. Por lo tanto, mientras que no se den de forma conjunta los requisitos del tipo penal (existencia de ánimo de lucro y el perjuicio de terceros), el simple hecho de descargarse archivos, no será una conducta tipificada como delito.

PATRICIA GABEIRAS / Estudios Jurídicos

NO

"La reforma no se refiere a Internet, ni su fin es ampliar el tipo delictivo a las descargas realizadas por este medio. El legislador simplemente ha aclarado y concretado que, si la reproducción o comunicación pública de la obra no ha sido consentida por su titular, el delito de importación ilegal también se cometerá aun cuando el producto se haya adquirido legalmente en el país origen de la importación. Por tanto, al igual que ocurría antes del 1 de octubre, la cuestión será determinar qué hay que entender por actividad de "importación" y cuándo ésta es "intencionada".

PALOMA LLANEZA / Llaneza y Asociados

NO

"Tras el 1 de octubre, se sigue penalizando la venta de CD y DVD piratas, al no haberse modificado la exigencia del ánimo de lucro para diferenciar el delito del ilícito civil, entre lo legal -la realización de copias para autoconsumo- de lo delictivo -la realización de copias con fines comerciales-. Ahora bien, se ha incorporado como nuevo delito la supresión de la protección de las grabaciones. La copia privada está autorizada, con lo que se puede desproteger un CD para uso personal. La cuestión es determinar si la desprotección para ofrecer o prestar música en una red p2p, aunque sea de manera gratuita, está autorizada también por la ley".

MARTÍ MANENT / derecho.com

NO

"Para que sea delito es necesario que el que realiza la descarga lo haga con ánimo de lucro y en perjuicio de un tercero. A mi entender, el ánimo de lucro consiste en obtener un beneficio patrimonial, un plus, y eso no puede equipararse con el conseguir una canción utilizando un programa de intercambio de archivos. En todo caso, descargarse canciones sin disponer de los correspondientes derechos de propiedad intelectual no es legal; sería un ilícito civil por vulneración de los derechos de propiedad intelectual. Es muy importante aclarar que el hecho de que bajarse música por la Red no sea un delito no quiere decir que sea legal".

CARLOS SÁNCHEZ-ALMEIDA / JAVIER MAESTRE / Bufete Sánchez Almeida

NO

"Descargarse música por Internet no es delito, si no hay ánimo de lucro. Según el artículo 270 del nuevo Código Penal, es delito reproducir, con ánimo de lucro y en perjuicio de un tercero, en todo o en parte, obras protegidas por derechos de autor sin la autorización de estos. La descarga de contenidos P2P no es delictiva en sí misma; sólo lo es si dicha reproducción persigue como finalidad un beneficio económico. El ánimo de lucro exigido por el Código Penal debe entenderse en sentido restrictivo, de acuerdo con la jurisprudencia más avanzada".

Alguna sentencia: caso elitedivx

Auto del Juzgado de Instrucción N. 4 de Cartagena, de diecisiete de abril de dos mil ocho, Proc. Abrev. 665 /2007,

extractos

…

…

Concisamente, la conducta desarrollada por los dos imputados mencionados habría consistido en la constitución y administración de la página web elitedivx.com, a través de la cual se daba acceso a unos programas de intercambio de *archivos peer to peer*, concretamente *emule* y *eDonkey*, de manera que los distintos usuarios de la página podían o llevaban a cabo el intercambio gratuito de diferentes obras audiovisuales con otros usuarios. En el desarrollo de esta actividad los imputados citados no intervienen directamente sobre las obras, salvo en lo tocante a actuaciones de tipo técnico y de control, y no obtenían una ganancia directa proveniente del acceso a la página web o de las obras que serían intercambiadas, con independencia de la ganancia que pudieron obtener de la publicidad insertada en la citada página y de la participación en la gestión de la misma.

Aunque éste no sea lugar para analizarlo, podría entenderse que tales tipos de actividades podrían suponer, desde la óptica del Ordenamiento extra—penal, una vulneración de los derechos de explotación de los titulares de los derechos de propiedad intelectual existentes sobre las obras afectadas, al suponer una actuación de intermediación en la comunicación pública de las obras en cuestión.

Ante la cuestión de si esa labor de mera intermediación tiene o no trascendencia penal parece claro que no es así. Siendo que la Ley 34/2.002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico ya establece importantes límites, a efectos de responsabilidad de los intermediadores, no tendría justificación que la mera actividad de intermediación fuera perseguida penalmente. Concretamente, digamos, a efectos ilustrativos, que el artículo 14 de la mencionada Ley establece que los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir datos facilitados por el destinatario del servicio o en facilitar el acceso a ésta no son responsables por la información transmitida, salvo que hayan originado la transmisión o modificado los datos o seleccionado éstos o sus destinatarios, no entendiéndose modificación la manipulación técnica de los archivos que alberguen los datos, que tenga lugar durante la transmisión. Asi mismo, el artículo 17 de tal Ley dice que 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 serán responsables por la información a que dirijan a los destinatarios de sus servicios, siempre que no tengan conocimiento efectivo de que la actividad o la información en cuestión son ilícitas o que lesionan bienes o derechos de un tercero susceptibles de indemnización, entendiéndose que tiene ese conocimiento cuando un órgano competente haya declarado la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos, o hubiera declarado la existencia de la lesión y el prestador conociera la correspondiente resolución.

Descartado que las meras labores de intermediación en la comunicación pública de obras a través de internet sin autorización de los titulares de los respectivos derechos de propiedad intelectual tenga trascendencia penal o asumiendo, a lo sumo, que puede tenerla si el imputado interviene, además, sobre el contenido de los archivos de forma fundamental, cabe examinar si la conducta a la que se viene haciendo referencia puede considerarse una comunicación pública a los efectos del artículo 270 del Código Penal. La respuesta aquí ha de ser también negativa: es cierto que el tipo citado no lo es en blanco, pero como si lo fuera, dado que la cantidad de elementos normativos que contiene lleva a integrar su regulación con la que en otras ramas del Ordenamiento definen las conductas en cuestión. Esto no puede llevar a entender que todos los supuestos previstos en la norma extra—penal tengan encaje en el tipo, por cuanto lo contrario podría producir el efecto no deseado de solapar ambos ámbitos de protección. En lo que afecta, en concreto, a los actos de "comunicación pública" de la obra cabe acudir al artículo 20 del R.D. Legislativo 1/1996 de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. Tal precepto dice que se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares, no considerándose pública la que se celebre en el ámbito estrictamente doméstico que no esté conectado a una red de difusión de cualquier tipo. Esta definición general contenida en el. punto 1 del precepto se detalla el 2, en el que se establece que "especialmente son actos de comunicación pública..." los que se enumeran a continuación. **Para que un acto de comunicación pública concreto pudiese tener trascendencia penal debería,** al menos, verse integrado en el catálogo referido, por cuanto lo contrario podría afectar al principio de taxatividad penal, dada la amplitud e inconcreción de que adolece el punto 1 del citado artículo 20. Dicho lo cual, ha de tenerse en cuenta que una conducta como la que se viene examinando sólo tiene cabida en la letra i) del citado artículo 20.2 (en éste se habla de "*La puesta a disposición del público de obras, por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elije.*"), siendo que tal apartado fue integrado en el citado precepto después de ocurrir los hechos, que se retrotraen, como fecha límite máxima, al primer semestre de 2.006, y a posibles fechas anteriores, resultando que el citado apartado 1) entró en vigor con fecha de 28—7—2.006, en virtud de la reforma operada por la Ley 23/2.006 de 7 de julio. Por lo tanto, su vigencia es posterior a la fecha de los hechos.

Existen dos últimos aspectos a tomar en consideración, cuales son los elementos del tipo analizado consistentes en que los hechos han de llevarse a cabo con "ánimo de lucro" y **"en perjuicio de tercero"**. Aunque sobre este último particular existen dos tendencias doctrinales, la que considera que se trata de un elemento objetivo del tipo, que lleva a resaltar una mera tendencia que no exige para la consumación de la conducta un perjuicio efectivo y la que entiende que se trata de un elemento subjetivo, lo que conlleva que la consumación de la conducta no se produzca sino cuando se produce un perjuicio efectivo, hemos de decantarnos por esta última dado que lleva a un resultado más acorde con los principios penales primeramente citados y dado que entra mejor en consonancia con el tipo de derechos de autor protegidos penalmente, que son esencialmente derechos relacionados con la exclusividad en la explotación de obra. En un caso como el de autos no existe un perjuicio real y directo por cuanto no media contraprestación alguna que acompañe a la comunicación pública de la que se trataría,

siendo esta una tesis seguida por la SAP de Murcia (Secc. 59 de 24—4—2.006, al decir: "*d) Que tales conductas irroguen un perjuicio de tercero, titular de los derechos de propiedad intelectual, y que se presume cuando la reproducción, el plagio, la distribución y la comunicación pública se hace mediante un precio que evidencia la ganancia dejada de obtener por aquél. "*.

En lo que toca al **ánimo de lucro**, ha de entenderse que este elemento intencional del tipo pone de manifiesto que la conducta ha de ir acompañada del dolo específico de obtener una ganancia procedente del acto correspondiente que se realiza por el autor de la conducta realizada sin autorización. Los propios pormenores del tipo, según se desprende de los principios antes referidos, y de lo destacado en el párrafo anterior, llevan a entender que ese dolo ha de ser directo, es decir directamente ha de pretenderse obtener una ganancia a través de todas y cada una de las comunicaciones públicas de la obra u obras de que se trate, pretendiendo con ello, además, perjudicar al titular de tales derechos. Ese ánimo, según destaca la Circular 1/2.006 de la Fiscalía General del Estado ha de ser un ánimo de tipo comercial, lo que no se da cuando, como en el presente caso, quien intermedia en los actos de comunicación pública no obtiene un beneficio económico procedente de la intermediación en la comunicación de las distintas obras, sino que obtiene sus beneficios de otro modo, a través de la inserción de publicidad en la página web en la que se encuentran los programas de intermediación.

En consecuencia, en virtud de los principios penales de intervención mínima y proporcionalidad, en virtud de que los autos de intermediación en la comunicación de obras protegidas por derechos de autor no encajan en el tipo penal en tanto en cuanto quien intermedia no incida sobre las obras, en virtud de que un acto de intermediación como el de autos no se puede considerar como un acto de comunicación pública de conformidad con el principio de taxatividad penal, en virtud de que la conducta de autos no conlleva la producción de un perjuicio efectivo, real y directo sobre los titulares de los derechos protegidos y en virtud de que tal conducta no se ve guiada por un ánimo de lucro comercial tendente a la obtención de beneficios procedentes de la comunicación pública de las obras, dado que el beneficio no viene de los actos de comunicación sino de la inserción de publicidad en los canales de intermediación dispuestos para que se realice la comunicación, es por lo que procede acordar el sobreseimiento libre de la presente causa respecto a los hechos en ella imputados a F.T. y a D. M. L. L

VISTOS el precepto legal citado y de los demás de general y pertinente aplicación al caso,

EL MAGISTRADO—JUEZ

D. FRANCISCO JAVIER DE LA TORRE GUZMAN

D I S P O N E:

El sobreseimiento libre de las presentes actuaciones respecto a los hechos imputados a F. T. y a D. M. L. L., y el archivo de las mismas, notificándose la presente resolución al Sr. Fiscal y a las partes personadas, haciéndoles constar que cabe recurso de reforma en el plazo de tres días ante este Juzgado, así como recurso directo de apelación en plazo de 5 días ante la Audiencia provincial.

Así, por este auto, lo pronuncio, mando y lo firmo.

3. Falsedades.

Concepto de documento como todo soporte material que exprese o incorpore datos.

Extensión de la falsificación de moneda a las tarjetas de débito y crédito.

Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.

(Artículos 386 y ss. del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 386.

«Será castigado con la pena de prisión de ocho a 12 años y multa del tanto al décuplo del valor aparente de la moneda:

- 1.º El que altere la moneda o fabrique moneda falsa.
- 2.º El que introduzca en el país o exporte moneda falsa o alterada.
- 3.º El que transporte, expenda o distribuya, en connivencia con el falsificador, alterador, introductor o exportador, moneda falsa o alterada.

La tenencia de moneda falsa para su expendición o distribución será castigada con la pena inferior en uno o dos grados, atendiendo al valor de aquélla y al grado de connivencia con los autores mencionados en los números anteriores. La misma pena se impondrá al que, sabiéndola falsa, adquiera moneda con el fin de ponerla en circulación.

El que habiendo recibido de buena fe moneda falsa la expenda o distribuya después de constarle su falsedad será castigado con la pena de prisión de tres a seis meses o multa de seis a 24 meses, si el valor aparente de la moneda fuera superior a 400 euros.

Si el culpable perteneciere a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de estas actividades, el juez o tribunal podrá imponer alguna o algunas de las consecuencias previstas en el artículo 129 de este Código.

Artículo 387.

«A los efectos del artículo anterior, se entiende por moneda la metálica y papel moneda de curso legal. A los mismos efectos, se considerarán moneda las tarjetas de crédito, las de débito y las demás tarjetas que puedan utilizarse como medio de pago, así como los cheques de viaje. Igualmente, se equipararán a la moneda nacional las de otros países de la Unión Europea y las extranjeras.

Artículo 388.

La condena de un Tribunal extranjero impuesta por delito de la misma naturaleza de los comprendidos en este capítulo, será equiparada a las sentencias de los Jueces o

Tribunales españoles a los efectos de reincidencia, salvo que el antecedente penal haya sido cancelado o pudiese serlo con arreglo al Derecho español.

Artículo 389.

«El que falsificare o expendiere, en connivencia con el falsificador, sellos de correos o efectos timbrados, o los introdujera en España conociendo su falsedad, será castigado con la pena de prisión de seis meses a tres años.

El adquirente de buena fe de sellos de correos o efectos timbrados que, conociendo su falsedad, los distribuyera o utilizara en cantidad superior a 400 euros será castigado con la pena de prisión de tres a seis meses o multa de seis a 24 meses.

Artículo 390.

1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad:

1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.

2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.

3.º Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho.

4.º Faltando a la verdad en la narración de los hechos.

2. Será castigado con las mismas penas a las señaladas en el apartado anterior el responsable de cualquier confesión religiosa que incurra en alguna de las conductas descritas en los números anteriores, respecto de actos y documentos que puedan producir efecto en el estado de las personas o en el orden civil.

Artículo 391.

La autoridad o funcionario público que por imprudencia grave incurriere en alguna de las falsedades previstas en el artículo anterior o diere lugar a que otro las cometa, será castigado con la pena de multa de seis a doce meses y suspensión de empleo o cargo público por tiempo de seis meses a un año.

Artículo 392.

El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses.

Artículo 393.

El que, a sabiendas de su falsedad, presentare en juicio o, para perjudicar a otro, hiciere uso de un documento falso de los comprendidos en los artículos precedentes, será castigado con la pena inferior en grado a la señalada a los falsificadores.

Artículo 394.

1. La autoridad o funcionario público encargado de los servicios de telecomunicación que supusiere o falsificare un despacho telegráfico u otro propio de

dichos servicios, incurrirá en la pena de prisión de seis meses a tres años e inhabilitación especial por tiempo de dos a seis años.

2. El que, a sabiendas de su falsedad, hiciere uso del despacho falso para perjudicar a otro, será castigado con la pena inferior en grado a la señalada a los falsificadores.

Artículo 395.

El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años.

Artículo 396.

El que, a sabiendas de su falsedad, presentare en juicio o, para perjudicar a otro, hiciere uso de un documento falso de los comprendidos en el artículo anterior, incurrirá en la pena inferior en grado a la señalada a los falsificadores.

Artículo 397.

El facultativo que librare certificado falso será castigado con la pena de multa de tres a doce meses.

Artículo 398.

La autoridad o funcionario público que librare certificación falsa será castigado con la pena de suspensión de seis meses a dos años.

Artículo 399.

1. El particular que falsificare una certificación de las designadas en los artículos anteriores será castigado con la pena de multa de tres a seis meses.

2. La misma pena se aplicará al que hiciere uso, a sabiendas, de la certificación falsa.

Artículo 400.

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

4. Sabotajes informáticos.

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 263.

«El que causare daños en propiedad ajena no comprendidos en otros títulos de este Código, será castigado con la pena de multa de seis a 24 meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de 400 euros.

Artículo 264.

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2.º Que se cause por cualquier medio infección o contagio de ganado.

3.º Que se empleen sustancias venenosas o corrosivas.

4.º Que afecten a bienes de dominio o uso público o comunal.

5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

6.º La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

(POSIBLE REFORMA EN 2010)

"1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas informáticos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.º Se hubiese cometido en el marco de una organización criminal.

2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

4. Cuando de los delitos comprendidos en este artículo fuere responsable una persona jurídica de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3."

Artículo 625.

« 1.Serán castigados con la pena de localización permanente de dos a 12 días o multa de 10 a 20 días los que intencionadamente causaran daños cuyo importe no exceda de 400 euros.

2.Se impondrá la pena en su mitad superior si los daños se causaran en los lugares o bienes a que refiere el artículo 323 de este Código.

5. Fraudes informáticos.

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 248.

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

» Octogésimo segundo. Se añade un apartado 3 al artículo 248, que queda redactado como sigue:

« 3.La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo.

Artículo 249.

» Octogésimo tercero. Se modifica el artículo 249, que queda redactado como sigue:

«Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Artículo 250.

1.- El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:

1º Recaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.

2º Se realice con simulación de pleito o empleo de otro fraude procesal.

3º Se realice mediante cheque, pagaré, letra de cambio en blanco o negocio cambiario ficticio.

4º Se perpetre abusando de firma de otro, o sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, protocolo o documento público u oficial de cualquier clase.

5º Recaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.

6º Revista especial gravedad, atendiendo al valor de la defraudación, a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia.

7º Se cometa abuso de las relaciones personales existentes entre la víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional.

2.- Si concurrieran las circunstancias 6ª o 7ª con la 1ª del número anterior, se impondrán las penas de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

Artículo 251.

Será castigado con la pena de prisión de uno a cuatro años:

1º Quien, atribuyéndose falsamente sobre una cosa mueble o inmueble facultad de disposición de la que carece, bien por no haberla tenido nunca, bien por haberla ya ejercitado, la enejenare, gravare o arrendare a otro, en perjuicio de éste o de tercero.

2º El que dispusiere de una cosa mueble o inmueble ocultando la existencia de cualquier carga sobre la misma, o el que, habiéndola enejenado como libre, la gravare o enajenare nuevamente antes de la definitiva transmisión a adquiriente, en perjuicio de éste, o de un tercero.

3º El que otorgare en perjuicio de otro un contrato simulado.

artículo 252

«Serán castigados con las penas del artículo 249 ó 250, en su caso, los que en perjuicio de otro se apropiaren o distrajeren dinero, efectos, valores o cualquier otra cosa mueble o activo patrimonial que hayan recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarlos o devolverlos, o negaren haberlos recibido, cuando la cuantía de lo apropiado exceda de cuatrocientos euros. Dicha pena se impondrá en su mitad superior en el caso de depósito necesario o miserable.

Legislación en relación con las telecomunicaciones:

Art 255

» Octogésimo séptimo. Se modifica el primer párrafo del artículo 255, que queda redactado como sigue:

«Será castigado con la pena de multa de tres a 12 meses el que cometiere defraudación por valor superior a 400 euros, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1.- Valiéndose de mecanismo instalados para realizar la defraudación.
2.- Alterando maliciosamente las indicaciones o los aparatos contadores.
3.- Empleando cualesquiera otros medios clandestinos.

Art 256

» Octogésimo octavo. Se modifica el artículo 256, que queda redactado como sigue:

«El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.

259

» Octogésimo noveno. Se modifica el artículo 259, que queda redactado como sigue:

«Será castigado con la pena de uno a cuatro años de prisión y multa de 12 a 24 meses, el deudor que, una vez admitida a trámite la solicitud de concurso, sin estar autorizado para ello ni judicialmente ni por los administradores concursales, y fuera de los casos permitidos por la ley, realice cualquier acto de disposición patrimonial o generador de obligaciones, destinado a pagar a uno o varios acreedores, privilegiados o no, con posposición del resto.

artículo 286

« 1.Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

- 1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.
- 2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º

2.Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

3.A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.

4.A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación."

6. Amenazas.

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 169.

El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.

Artículo 170.

Si las amenazas de un mal que constituyere delito fuesen dirigidas a atemorizar a los habitantes de una población, grupo étnico, o a un amplio grupo de personas y tuvieran la gravedad necesaria para conseguirlo, se impondrán, respectivamente, las penas en grado a las previstas en al artículo anterior.

« 2.Serán castigados con la pena de prisión de seis meses a dos años, los que, con la misma finalidad y gravedad, reclamen públicamente la comisión de acciones violentas por parte de bandas armadas, organizaciones o grupos terroristas.

Artículo 171.

« 1.Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior.

2.Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será

castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere.

3.Si el hecho descrito en el apartado anterior consistiere en la amenaza de revelar o denunciar la comisión de algún delito el ministerio fiscal podrá, para facilitar el castigo de la amenaza, abstenerse de acusar por el delito cuya revelación se hubiere amenazado, salvo que éste estuviere castigado con pena de prisión superior a dos años. En este último caso, el juez o tribunal podrá rebajar la sanción en uno o dos grados.

7. Calumnias e injurias.

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

CÓDIGO PENAL

(L.O. 10/1995, de 23 de noviembre)

Artículo 205.

Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 206.

«Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses.

Artículo 207.

El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado.

Artículo 208.

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 209.

Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso con la de tres a siete meses.

Artículo 210.

El acusado de injuria quedará exento de responsabilidad probando la verdad de las imputaciones cuando éstas se dirijan contra funcionarios públicos sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de faltas penales o de infracciones administrativas.

Artículo 211.

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212.

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 213.

Si la calumnia o injuria fueren cometidas mediante precio, recompensa o promesa, los Tribunales impondrán, además de las penas señaladas para los delitos de que se trate, la de inhabilitación especial prevista en los artículos 42 ó 45 del presente Código, por tiempo de seis meses a dos años.

Artículo 214.

Si el acusado de calumnia o injuria reconociere ante la autoridad judicial la falsedad o falta de certeza de las imputaciones y se retractare de ellas, el Juez o Tribunal impondrá la pena inmediatamente inferior en grado y podrá dejar de imponer la pena de inhabilitación que establece el artículo anterior.

El Juez o Tribunal ante quien se produjera el reconocimiento ordenará que se entregue testimonio de retractación al ofendido y, si éste lo solicita, ordenará su publicación en el mismo medio en que se vertió la calumnia o injuria, en espacio idéntico o similar a aquél en que se produjo su difusión y dentro del plazo que señale el Juez o Tribunal sentenciador.

Artículo 215.

« 1.Nadie será penado por calumnia o injuria sino en virtud de querella de la persona ofendida por el delito o de su representante legal. Se procederá de oficio cuando la ofensa se dirija contra funcionario público, autoridad o agente de la misma sobre hechos concernientes al ejercicio de sus cargos.

2. Nadie podrá deducir acción de calumnia o injuria vertidas en juicio sin previa licencia del Juez o Tribunal que de él conociere o hubiere conocido.

3. El culpable de calumnia o injuria quedará exento de responsabilidad criminal mediante el perdón de la persona ofendida por el delito o de su representante legal, sin perjuicio de lo dispuesto en el segundo párrafo del número 4.º del artículo 130 de este Código.

Artículo 216.

En los delitos de calumnia o injuria se considera que la reparación del daño comprende también la publicación o divulgación de la sentencia condenatoria, a costa del condenado por tales delitos, en el tiempo y forma que el Juez o Tribunal consideren más adecuado a tal fin, oídas las dos partes.

8. Pornografía infantil.

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)

artículo 189,
« 1.Será castigado con la pena de prisión de uno a cuatro años:

- a) El que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades.
- b) El que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

2.El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

3.Serán castigados con la pena de prisión de cuatro a ocho años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

- a) Cuando se utilicen a niños menores de 13 años.
- b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio.
- c) Cuando los hechos revistan especial gravedad atendiendo al valor económico del material pornográfico.
- d) Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual.
- e) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.
- f) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho o de derecho, del menor o incapaz.

4.El que haga participar a un menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o desarrollo de la personalidad de éste, será castigado con la pena de prisión de seis meses a un año.

5.El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o incapaz y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o incapaz, será castigado con la pena de prisión de tres a seis meses o multa de seis a 12 meses.

6.El ministerio fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

7.Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por

cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada.

8.En los casos previstos en los apartados anteriores, se podrán imponer las medidas previstas en el artículo 129 de este Código cuando el culpable perteneciere a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

Otras reformas de interés LO 15/2003

» Décimo.Se modifica el artículo 48, que queda redactado como sigue:

« 1.La privación del derecho a residir en determinados lugares o acudir a ellos impide al penado residir o acudir al lugar en que haya cometido el delito, o a aquél en que resida la víctima o su familia, si fueren distintos.

2.La prohibición de aproximarse a la víctima, o a aquellos de sus familiares u otras personas que determine el juez o tribunal, impide al penado acercarse a ellos, en cualquier lugar donde se encuentren, así como acercarse a su domicilio, a sus lugares de trabajo y a cualquier otro que sea frecuentado por ellos, quedando en suspenso, respecto de los hijos, el régimen de visitas, comunicación y estancia que, en su caso, se hubiere reconocido en sentencia civil hasta el total cumplimiento de esta pena.

3.La prohibición de comunicarse con la víctima, o con aquellos de sus familiares u otras personas que determine el juez o tribunal, impide al penado establecer con ellas, por cualquier medio de comunicación o medio informático o telemático, contacto escrito, verbal o visual.

Cuestionario sobre delitos e internet

(SEÑALA, EN SU CASO, EL ARTÍCULO APLICABLE)

1- Está penada la interceptación del correo electrónico?

2- Está penado difundir los datos personales registrados en ficheros o soportes informáticos si se es quien ha cometido el acceso ilícito de los mismos?

3- En los anteriores delitos tiene diferente tratamiento que se tenga ánimo lucrativo o que simplemente se quiera poner en evidencia la seguridad de un servidor?

4- Está penado aprovechar los contenidos de otra página web para la tuya propia sin la autorización de quien sea su autor o tenga los derechos de tales contenidos

5- Almacenar en el disco duro del ordenador sin autorización obras -como las musicales- está penado? Razona tu respuesta.

6- La tenencia en tu disco duro de programas que te hayas bajado de la red destinados a desproteger programas de ordenador estaría penada?

7- Crees que la falsificación de la firma electrónica de un documento administrativo interno en dicho soporte puede ser calificada como delito.

8- Crees que la falsificación de la firma electrónica (en certificación avanzada con plena validez jurídica en virtud de la normativa vigente) puede ser calificada como delito?

9- Cómo calificar el típico acto de hacker de introducirse en una red alterando programas o domunentos?

10- En el apartado de fraudes, qué tipos penales consideras que pueden cometerse normalmente a través de la red.

11- Comenza el artículo 286 (ya vigente), conoces algún caso de posible comisión de este delito, coméntalo brevemente (sin datos concretos).

12- Si las amenazas se llevan a cabo a través de correo electrónico, se le aplicaría algún apartado específico de la legislación penal relativa a las mismas?

13- Si se comete injurias o calumnias en una página web se agrava de algún modo la responsabilidad?

14- La retractación o el fallo judicial puede ser publicada en una página web?

15- Está penada la tenencia de pornografía infantil en soporte informático, que por ejemplo, se haya „bajado" de la red.

16. Qué tipo-s relativo-s a la legislación penal sobre fraudes en telecomunicaciones crees que se puede cometer por un hacker?

17. Crees que bajarse música de internet a través de un programa p2p es delito? Y tener una web que facilita esta actividad?

Respecto de la resolución judicial del caso elitedivx

¿Cree el Juzgado que los hechos son posiblemente ilícitos?

¿Qué es comunicación pública de una obra según la legislación de propiedad intelectual?

Desde la perspectiva penal, que la cuestión es si se persigue por el artículo 270 c. penal. la comunicación pública de obras a través de internet sin autorización de los titulares de los respectivos derechos de propiedad intelectual es penalmente perseguible si el imputado interviene sobre el contenido de los archivos de forma fundamental.

¿Qué tendencias se afirman respecto de "en perjuicio de tercero" del artículo 270 c. penal?

¿Por cuál opta el juez?

¿Cómo entiende el juzgador "el ánimo de lucro"

¿Qué dice la Circular 1/2.006 de la Fiscalía General del Estado al respecto del ánimo de lucro.

¿Qué concluye finalmente?

IX. PROPIEDAD INTELECTUAL

1. Regulación básica

Toda la normativa está disponible, entre otros, en www.sgae.es
Española
REAL DECRETO LEGISLATIVO 1/1996, DE 12 DE ABRIL, por el que se aprueba el texto refundido de la ley de propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, modificado por la ley 5/1998 y ley 1/2000
http://constitucion.rediris.es/legis/1996/rdleg0001-1996.html

Relación de Directivas comunitarias que regulan las materias vinculadas

DIRECTIVA 91/250/CEE DEL CONSEJO de 14 de mayo de 1991 sobre la protección jurídica de programas de ordenador. ES DOCE 17.05.1991 L 122.

DIRECTIVA 92/100/CEE DEL CONSEJO de 19 de noviembre de 1992 sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual. ES DOCE 27.11.1992 L 346.

DIRECTIVA 93/83/CEE DEL CONSEJO de 27 de septiembre de 1993 sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor en el ámbito de la radiodifusión vía satélite y de la distribución por cable ES DOCE L 248 06.10.1993

DIRECTIVA 93/98/CEE DEL CONSEJO de 29 de octubre de 1993 relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines. ES DOCE 24.11.1993 L 290.

DIRECTIVA 96/9/CE DEL PARLAMENTO EUROPEO DEL CONSEJO de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos. ES DOCE 27.3.1996 L 77.

DIRECTIVA 98/71/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de octubre de 1998 sobre la protección jurídica de los dibujos y modelos.

DIRECTIVA 2001/29/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 22 de mayo de 2001 relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la Sociedad de la Información. ES DOCE 22.6.2001 L 167/10.

DIRECTIVA 2001/84/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de septiembre de 2001 relativa al derecho de participación en beneficio del autor de una obra de arte original. ES DOCE 13.10.2001 L 272/32.

2. Extractos de la Ley de propiedad intelectual

REAL DECRETO LEGISLATIVO 1/1996, DE 12 DE ABRIL, POR EL QUE SE APRUEBA EL TEXTO REFUNDIDO DE LA LEY DE PROPIEDAD INTELECTUAL, REGULARIZANDO, ACLARANDO Y ARMONIZANDO LAS DISPOSICIONES LEGALES VIGENTES SOBRE LA MATERIA.

De los derechos de autor.

Disposiciones generales.

Artículo 3. Características.

Los derechos de autor son independientes, compatibles y acumulables con:

• La propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual.

• Los derechos de propiedad industrial que puedan existir sobre la obra.

• Los otros derechos de propiedad intelectual reconocidos en el Libro II de la presente Ley.

Sujeto, objeto y contenido.

Sujetos.

Artículo 5. Autores y otros beneficiarios.

1. Se considera autor a la persona natural que crea alguna obra literaria, artística o científica.

2. No obstante, de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella.

Artículo 7. Obra en colaboración.

Artículo 8. Obra colectiva.

Objeto.

Artículo 10. Obras y Títulos originales.

1. Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:

Artículo 12. Colecciones. Bases de datos.

1. También son objeto de propiedad intelectual, en los términos del Libro I de la presente Ley, las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.

La protección reconocida en el presente artículo a estas colecciones se refiere únicamente a su estructura en cuanto forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos.

2. A efectos de la presente Ley, y sin perjuicio de lo dispuesto en el apartado anterior, se consideran bases 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.

3. La protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos.

Contenido

Artículo 14. Contenido y características del derecho moral.

Corresponden al autor los siguientes derechos irrenunciables e inalienables:

• Decidir si su obra ha de ser divulgada y en qué forma.

• Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.

• Exigir el reconocimiento de su condición de autor de la obra.

• Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación.

• Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.

• Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación.

• Si, posteriormente, el autor decide reemprender la explotación de su obra deberá ofrecer preferentemente los correspondientes derechos al anterior titular de los mismos y en condiciones razonablemente similares a las originarias.

• Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.

• Este derecho no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos incomodidades al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le irroguen.

Artículo 17. Derecho exclusivo de explotación y sus modalidades.

Corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley.

Artículo 18. Reproducción.

Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.

Artículo 19. Distribución.

1. Se entiende por distribución la puesta a disposición del público del original o de las copias de la obra, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

Artículo 20. Comunicación pública.

1. Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.

No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo.

2. Especialmente, son actos de comunicación pública:

a. La proyección o exhibición pública de las obras cinematográficas y de las demás audiovisuales.

b. La emisión de cualesquiera obras por radiodifusión o por cualquier otro medio que sirva para la difusión inalámbrica de signos, sonidos o imágenes. El concepto de emisión comprende la producción de señales portadoras de programas hacia un satélite, cuando la recepción de las mismas por el público no es posible sino a través de entidad distinta de la de origen.

c. La puesta a disposición del público de obras, por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija

d. El acceso público en cualquier forma a las obras incorporadas a una base de datos, aunque dicha base de datos no esté protegida por las disposiciones del Libro I de la presente Ley.

Artículo 21. Transformación.

1. La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.

Cuando se trate de una base de datos a la que hace referencia el artículo 12 de la presente Ley se considerará también transformación, la reordenación de la misma.

2. Los derechos de propiedad intelectual de la obra resultado de la transformación corresponderán al autor de esta última, sin perjuicio del derecho del autor de la obra preexistente de autorizar, durante todo el plazo de protección de sus derechos sobre ésta, la explotación de esos resultados en cualquier forma y en especial mediante su reproducción, distribución, comunicación pública o nueva transformación.

Artículo 22. Colecciones escogidas u obras completas.

La cesión de los derechos de explotación sobre sus obras no impedirá al autor publicarlas reunidas en colección escogida o completa.

Artículo 23. Independencia de derechos.

Los derechos de explotación regulados en esta sección son independientes entre sí.

Artículo 25. Compensación equitativa por copia privada.

1. La reproducción realizada exclusivamente para uso privado, mediante aparatos o instrumentos técnicos no tipográficos, de obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen reglamentariamente, así como de fonogramas, videogramas o de otros soportes sonoros, visuales o audiovisuales, originará una compensación equitativa y única por cada una de las tres modalidades de reproducción mencionadas, en favor de las personas que se expresan en el párrafo b del apartado 4, dirigida a compensar los derechos de propiedad intelectual que se dejaran de percibir por razón de la expresada reproducción. Este derecho será irrenunciable para los autores y los artistas, intérpretes o ejecutantes.

2. Esa compensación se determinará para cada modalidad en función de los equipos, aparatos y soportes materiales idóneos para realizar dicha reproducción, fabricados en territorio español o adquiridos fuera de éste para su distribución comercial o utilización dentro de dicho territorio.

3. Lo dispuesto en los apartados anteriores no será de aplicación a los programas de ordenador ni a las bases de datos electrónicas.

6. Para los equipos, aparatos y soportes materiales de reproducción digitales, el importe de la compensación que deberá satisfacer cada deudor será el que se apruebe conjuntamente por los Ministerios de Cultura y de Industria, Turismo y Comercio, conforme a las siguientes reglas:

Ministerio de la Presidencia (BOE n. 148 de 19/6/2008)

ORDEN PRE/1743/2008, de 18 de junio, por la que se establece la relación de equipos, aparatos y soportes materiales sujetos al pago de la compensación equitativa por copia privada, las cantidades aplicables a cada uno de ellos y la distribución entre las diferentes modalidades de reproducción.

http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2008/10443

Duración, límites y salvaguardia de otras disposiciones legales

Duración

Artículo 26. Duración y cómputo.

Los derechos de explotación de la obra durarán toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento.

Límites

Artículo 31. Reproducciones provisionales y copia privada.

1. No requerirán autorización del autor los actos de reproducción provisional

sean transitorios o accesorios y formen parte integrante y esencial de un proceso tecnológico y cuya única finalidad consista en facilitar bien una transmisión en red entre terceras partes por un intermediario

persona física para su uso privado a partir de obras a las que haya accedido legalmente y la copia obtenida no sea objeto de una utilización colectiva ni lucrativa, sin perjuicio de la compensación equitativa prevista en el artículo 25

Quedan excluidas de lo dispuesto en este apartado las bases de datos electrónicas y, en aplicación del artículo 99.a, los programas de ordenador.

2. No necesita autorización del autor la reproducción, en cualquier soporte, de obras ya divulgadas cuando se lleve a cabo por una **persona física para su uso privado a partir de obras a las que haya accedido legalmente y la copia obtenida no sea objeto de una utilización colectiva ni lucrativa, sin perjuicio de la compensación equitativa prevista en el artículo 25**, que deberá tener en cuenta si se aplican a tales obras las medidas a las que se refiere el artículo 161. **Quedan excluidas de lo dispuesto en este apartado las bases de datos electrónicas y, en aplicación del artículo 99.a, los programas de ordenador.**

Excepciones de autorización del autor

Artículo 31 bis. Seguridad, procedimientos oficiales y discapacidades.

2. Tampoco necesitan autorización

en beneficio de personas con discapacidad, siempre que los mismos carezcan de finalidad lucrativa,

Artículo 32. Cita e ilustración de la enseñanza.

Es lícita la inclusión en una obra propia de fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como la de obras aisladas de carácter plástico o fotográfico figurativo, siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico.

sólo fines docentes o de investigación,

32. 2. Las recopilaciones periódicas efectuadas en forma de reseñas o revista de prensa tendrán la consideración de citas. No obstante, cuando se realicen recopilaciones de artículos periodísticos que consistan básicamente en su mera reproducción y dicha actividad se realice con fines comerciales, el autor que no se haya opuesto expresamente tendrá derecho a percibir una remuneración equitativa. **En caso de oposición expresa del autor, dicha actividad no se entenderá amparada por este límite.**

2. No necesitará autorización del autor el profesorado de la educación reglada

cuando tales actos se hagan únicamente para la ilustración de sus actividades educativas en las aulas

INTERNET ¿Artículo 33. Trabajos sobre temas de actualidad.

1. Los trabajos y artículos sobre temas de actualidad difundidos por los medios de comunicación social podrán ser reproducidos, distribuidos y comunicados públicamente por cualesquiera otros de la misma clase, citando la fuente y el autor si el trabajo apareció con firma y siempre que no se hubiese hecho constar en origen la reserva de derechos. Todo ello sin perjuicio del derecho del autor a percibir la remuneración acordada o, en defecto de acuerdo, la que se estime equitativa.

Cuando se trate de colaboraciones literarias será necesaria, en todo caso, la oportuna autorización del autor.

conferencias, alocuciones, informes ante los Tribunales

Artículo 34. Utilización de bases de datos por el usuario legítimo y limitaciones a los derechos de explotación del titular de una base de datos.

Artículo 37. Reproducción, préstamo y consulta de obras mediante terminales especializados en determinados establecimientos.

Los titulares de estos establecimientos remunerarán a los autores por los préstamos que realicen de sus obras en la cuantía que se determine mediante Real Decreto. La remuneración se hará efectiva a través de las entidades de gestión de los derechos de propiedad intelectual.

3. No necesitará autorización del autor la comunicación de obras o su puesta a disposición de personas concretas del público a efectos de investigación cuando se realice mediante red cerrada e interna a través de terminales especializados instalados a tal efecto en los locales de los establecimientos citados en el anterior apartado y siempre que tales obras figuren en las colecciones del propio establecimiento y no sean objeto de condiciones de adquisición o de licencia. Todo ello sin perjuicio del derecho del autor a percibir una remuneración equitativa

Artículo 39. Parodia.

Artículo 40 bis. Disposición común a todas las del presente capítulo.

Los artículos del presente capítulo no podrán interpretarse de manera tal que permitan su aplicación de forma que causen un perjuicio injustificado a los intereses legítimos del autor o que vayan en detrimento de la explotación normal de las obras a que se refieran.

Salvaguardia de aplicación de otras disposiciones legales.

Transmisión de los derechos

Disposiciones generales

Artículo 43. Transmisión inter vivos.

1. Los derechos de explotación de la obra pueden transmitirse por actos inter vivos, quedando limitada la cesión al derecho o derechos cedidos, a las modalidades de explotación expresamente previstas y al tiempo y ámbito territorial que se determinen.

2. La falta de mención del tiempo limita la transmisión a cinco años y la del ámbito territorial al país en el que se realice la cesión. Si no se expresan

específicamente y de modo concreto las modalidades de explotación de la obra, la cesión quedará limitada a aquella que se deduzca necesariamente del propio contrato y sea indispensable para cumplir la finalidad del mismo.

3. Será nula la cesión de derechos de explotación respecto del conjunto de las obras que pueda crear el autor en el futuro.

4. Serán nulas las estipulaciones por las que el autor se comprometa a no crear alguna obra en el futuro.

5. La transmisión de los derechos de explotación no alcanza a las modalidades de utilización o medios de difusión inexistentes o desconocidos al tiempo de la cesión.

Contrato de edición

Contrato de representación teatral y ejecución musical

Obras cinematográficas y demás obras audiovisuales

Programas de ordenador

Artículo 95. Régimen jurídico.

El derecho de autor sobre los programas de ordenador se regirá por los preceptos del presente Título y, en lo que no esté específicamente previsto en el mismo, por las disposiciones que resulten aplicables de la presente Ley.

Artículo 96. Objeto de la protección.

1. A los efectos de la presente Ley se entenderá por programa de ordenador 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.

A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador.

2. El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.

4. No estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces.

Derecho sui generis sobre las bases de datos.

Artículo 133. Objeto de protección.

1. El derecho sui generis sobre una base de datos protege la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido.

puede prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, siempre que

la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo.

a. Extracción, la transferencia permanente o temporal de la totalidad o de una parte sustancial del contenido de una base de datos a otro soporte cualquiera que sea el medio utilizado o la forma en que se realice.

b. Reutilización, toda forma de puesta a disposición del público de la totalidad o de una parte sustancial del contenido de la base mediante la distribución de copias en forma de venta u otra transferencia de su propiedad o por alquiler, o mediante transmisión en línea o en otras formas. A la distribución de copias en forma de venta en el ámbito de la Unión Europea le será de aplicación lo dispuesto en el apartado 2 del artículo 19 de la presente Ley.

Artículo 134. Derechos y obligaciones del usuario legítimo.

1. El fabricante de una base de datos, sea cual fuere la forma en que haya sido puesta a disposición del público, no podrá impedir al usuario legítimo de dicha base extraer y/o reutilizar partes no sustanciales de su contenido, evaluadas de forma cualitativa o cuantitativa, con independencia del fin a que se destine.

Artículo 135. Excepciones al derecho sui generis.

1. El usuario legítimo de una base de datos, sea cual fuere la forma en que ésta haya sido puesta a disposición del público, podrá, sin autorización del fabricante de la base, extraer y/o reutilizar una parte sustancial del contenido de la misma, en los siguientes casos:

a. Cuando se trate de una extracción para fines privados del contenido de una base de datos no electrónica.

b. Cuando se trate de una extracción con fines ilustrativos de enseñanza o de investigación científica en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente.

c. Cuando se trate de una extracción y/o reutilización para fines de seguridad pública o a efectos de un procedimiento administrativo o judicial.

2. Las disposiciones del apartado anterior no podrán interpretarse de manera tal que permita su aplicación de forma que cause un perjuicio injustificado a los intereses legítimos del titular del derecho o que vaya en detrimento de la explotación normal del objeto protegido.

De la protección de los derechos reconocidos en esta ley

Acciones y procedimientos

Artículo 138. Acciones y medidas cautelares urgentes.

El titular de los derechos reconocidos en esta Ley, sin perjuicio de otras acciones que le correspondan, podrá instar el cese de la actividad ilícita del infractor y exigir la indemnización de los daños materiales y morales causado

las medidas de cesación específicas contempladas en el artículo 139.1.h como las medidas cautelares previstas

podrán también solicitarse, cuando sean apropiadas, contra los intermediarios a cuyos servicios recurra un tercero para infringir derechos de propiedad intelectual reconocidos en esta ley, aunque los actos de dichos intermediarios no constituyan en sí mismos una infracción

Dichas medidas habrán de ser objetivas, proporcionadas y no discriminatorias.

a. La suspensión de la explotación o actividad infractora, incluyendo todos aquellos actos o actividades a los que se refieren los artículos 160 y 162.

b. La prohibición al infractor de reanudar la explotación o actividad infractora.

c. La remoción o el precinto de los aparatos utilizados en la comunicación pública no autorizada de obras o prestaciones, así como de aquellas en las que se haya suprimido o alterado sin autorización la información para la gestión electrónica de derechos, en los términos previstos en el artículo 162, o a las que se haya accedido eludiendo su protección tecnológica, en los términos previstos en el artículo 160.

d. El comiso, la inutilización y, en caso necesario, la destrucción de los instrumentos, con cargo al infractor, cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador. Las mismas medidas podrán adoptarse en relación con los dispositivos, productos o componentes para la elusión de medidas tecnológicas a los que se refiere el artículo 160 y para suprimir o alterar la información para la gestión electrónica de derechos a que se refiere el artículo 162.

e. La suspensión de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual, sin perjuicio de lo dispuesto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Artículo 140. Indemnización.

1. La indemnización por daños y perjuicios debida al titular del derecho infringido comprenderá no sólo el valor de la pérdida que haya sufrido, sino también el de la ganancia que haya dejado de obtener a causa de la violación de su derecho. La cuantía indemnizatoria podrá incluir, en su caso, los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial.

2. La indemnización por daños y perjuicios se fijará, a elección del perjudicado, conforme a alguno de los criterios siguientes:

a. Las consecuencias económicas negativas, entre ellas la pérdida de beneficios que haya sufrido la parte perjudicada y los beneficios que el infractor haya obtenido por la utilización ilícita.

En el caso de daño moral procederá su indemnización, aun no probada la existencia de perjuicio económico. Para su valoración se atenderá a las circunstancias de la infracción, gravedad de la lesión y grado de difusión ilícita de la obra.

b. La cantidad que como remuneración hubiera percibido el perjudicado, si el infractor hubiera pedido autorización para utilizar el derecho de propiedad intelectual en cuestión.

3. La acción para reclamar los daños y perjuicios a que se refiere este artículo prescribirá a los cinco años desde que el legitimado pudo ejercitarla.

Artículo 141. Medidas cautelares.

3. Cláusulas típicas de exención en sitios más que dudosamente lícitos

La copia de software o cualquier obra intelectual sin ánimo de lucro no constituye delito, habiéndose pronunciado en dicho sentido los jueces españoles en reiteradas sentencias.

La visita o acceso a esta página web, que es de carácter privado y no público, exige la aceptación del presente aviso. En esta web se podrá acceder a una programación PHP que es utilizada por los usuarios para la publicación de diversa información relacionada con el mundo de las redes P2P. El único material que existe en la web es el proporcionado por sus usuarios y colaboradores, que son plenamente responsables de los contenidos que publiquen en elitedivx, que no necesariamente ha de compartir dichas opiniones e información. Por tanto, elitedivx no tiene responsabilidad en cuanto a las informaciones, opiniones y enlaces que se publiquen. elitedivx no se hace responsable de aquellos otros sitios web u archivos a los que sea posible acceder a través de enlaces de hipertexto (links ó elinks) disponibles entre dichos contenidos, dado que dichas páginas y archivos enlazados son responsabilidad de sus respectivos titulares, ni han sido suministrados por elitedivx, sino por sus usuarios. Por consiguiente elitedivx ni aprueba, ni hace suyos los productos, servicios, contenidos, información, datos, opiniones archivos y cualquier clase de material existente en tales páginas web y no controla ni se hace responsable de la calidad, licitud, fiabilidad y utilidad de la información, contenidos y servicios existentes en los sitios y archivos enlazados y que son ajenos a esta página.

En el caso de que así se estime oportuno o le sea requerido por orden judicial o administrativa, elitedivx eliminará los enlaces a aquellas páginas web o archivos que infrinjan la legalidad.

Ninguna de las más de 50 personas que componen el equipo de la página recibe beneficio alguno por validar, moderar o introducir los enlaces que los usuarios envían o los mensajes que dejan. La poca publicidad que posee el sitio es para costear el alto gasto en transferencia y servidores dedicados que la página requiere , hecho que se podrá demostrar si llegase a ser necesario .

elitedivx está en contra de la piratería y reprueba cualquier comportamiento ilícito y contrario a los derechos de propiedad intelectual o de otra índole. El usuario se compromete a hacer un uso adecuado y lícito del sitio web y de sus contenidos, de conformidad con la Legislación aplicable, el presente aviso, la moral y buenas costumbres generalmente aceptadas y el orden público. De esta forma, el usuario deberá abstenerse de hacer un uso no autorizado o fraudulento del website y/o de los contenidos con fines o efectos ilícitos, así como de introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar daños en los sistemas físicos o lógicos de la página, de sus proveedores o de terceros.

Esta página es de carácter gratuito y privado. Por ello el acceso a la misma puede estar restringido, reservándose el derecho de admisión y, por consiguiente, no somos responsables de disfunciones o fallos en el acceso o visualización de la página.

El acceso a la totalidad del contenido de la página esta abierto a todo el mundo, sin obligar al registro de las personas para obtener un beneficio fijo con ello.

Los jueces españoles se han pronunciado en reiteradas ocasiones a favor del derecho de copia privada, como puede consultarse en estas sentencias.

La entrada en la Web implica la aceptación de estas condiciones, de lo contrario no estás autorizado a entrar.

****

Este Foro no contiene ningún tipo de archivo, todo esta basado en programas p2p tipo Emule, Edonkey y Overnet. Este Foro solo contiene los enlaces que nos envían los usuarios y colaboradores, solo ellos son los responsables de dichos enlaces. La Administración de este Foro, así como sus moderadores, no tienen ninguna responsabilidad de los comentarios, imágenes o enlaces que sea posible acceder a través de hipertextos. Ninguna persona de las que componen este Foro recibe beneficio alguno por moderar o introducir los enlaces que envían los usuarios.

****

AVISO IMPORTANTE

-La copia de software o cualquier obra intelectual sin ánimo de lucro no constituye delito, habiéndose pronunciado en dicho sentido los jueces españoles en reiteradas sentencias.

-La visita o acceso a esta página web, que es de carácter privado y no público, exige la aceptación del presente aviso. En esta web se podrá acceder a una programación PHP que es utilizada por los usuarios para la publicación de diversa información relacionada con el mundo de las redes P2P. El único material que existe en la web es el proporcionado por sus usuarios y colaboradores, que son plenamente responsables de los contenidos que publiquen en eMule24horas, que no necesariamente ha de compartir dichas opiniones e información. Por tanto, eMule24horas no tiene responsabilidad en cuanto a las informaciones, opiniones y enlaces que se publiquen. eMule24horas no se hace responsable de aquellos otros sitios web u archivos a los que sea posible acceder a través de enlaces de hipertexto (links ó elinks) disponibles entre dichos contenidos, dado que dichas páginas y archivos enlazados son responsabilidad de sus respectivos titulares, ni han sido suministrados por eMule24horas,

sino por sus usuarios. Por consiguiente eMule24horas ni aprueba, ni hace suyos los productos, servicios, contenidos, información, datos, opiniones archivos y cualquier clase de material existente en tales páginas web y no controla ni se hace responsable de la calidad, licitud, fiabilidad y utilidad de la información, contenidos y servicios existentes en los sitios y archivos enlazados y que son ajenos a esta página.

-En el caso de que así se estime oportuno o le sea requerido por orden judicial o administrativa, eMule24horas eliminará los enlaces a aquellas páginas web o archivos que infrinjan la legalidad.

-eMule24horas está en contra de la piratería y reprueba cualquier comportamiento ilícito y contrario a los derechos de propiedad intelectual o de otra índole. El usuario se compromete a hacer un uso adecuado y lícito del sitio web y de sus contenidos, de conformidad con la Legislación aplicable, el presente aviso, la moral y buenas costumbres generalmente aceptadas y el orden público. De esta forma, el usuario deberá abstenerse de hacer un uso no autorizado o fraudulento del website y/o de los contenidos con fines o efectos ilícitos, así como de introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar daños en los sistemas físicos o lógicos de la página, de sus proveedores o de terceros.

-Esta página es de carácter gratuito y privado. Por ello el acceso a la misma puede estar restringido, reservándose el derecho de admisión y, por consiguiente, no somos responsables de disfunciones o fallos en el acceso o visualización de la página.

-Los jueces españoles se han pronunciado en reiteradas ocasiones a favor del derecho de copia privada, como puede consultarse en diversas sentencias.

-La entrada en la Web implica la aceptación de estas condiciones, de lo contrario no estás autorizado a entrar.

(- Este lugar es privado y de acceso restringido y por ello se encuentra bajo los derechos y la protección que a estos lugares las leyes de nuestro país, el Ordenamiento Jurídico Internacional y el el Internet Privacy Act dispensan, no pudiéndose entender que aceptamos la libre entrada.

- Los sujetos que deseen entrar en este Web-site deberán ser mayores de edad y estar en plena posesión de sus facultades o, en caso de minoría de edad, deberán contar con la aprobación de sus progenitores, tutores o aquella persona que mantenga la patria potestad sobre su persona. En caso contrario queda totalmente prohibida la entrada.

- Todas las marcas aquí mencionadas y símbolos están registrados por sus legítimos propietarios y solamente se emplean en referencia a las mismas y con un fin de cita o comentario, de acuerdo con el articulo 32 LPI.

- Usted como usuario de nuestro servicio, declara que emplea nuestro producto y servicios por decisión propia.

- Toda la información y programas aquí recogidos van destinados al efectivo cumplimiento de los derechos recogidos en el artículo 31 RD/ 1/1996 por el que se aprueba el texto refundido de la Ley de la Propiedad Intelectual (LPI) en especial referencia al artículo 31.2 LPI, y en concordancia con lo expresado en el artículo 100.2 de esta misma ley .

- En ningún caso esta página apoya la piratería, es más, la rechaza frontalmente.

- Si pretendes utilizar esta web y su material como epicentro de tus actos ilícitos e ilegales, te equivocas de lugar, y todo mal acto que hagas será responsabilidad tuya y en ningún caso de los webmasters.

- En ningún caso o circunstancia se podrá responsabilizar directamente o indirectamente al propietario ni a los colaboradores del ilícito uso de la información contenida en esta web-site. Así mismo tampoco se nos podrá responsabilizar directamente o indirectamente de incorrecto uso o mala interpretación que se haga de la información y servicios incluidos. Igualmente quedara fuera de nuestra responsabilidad el materia al que usted pueda acceder desde nuestros links. Expresando nuestra mas profunda creencia de que las web-site que tienen link en nuestra web cumplen plenamente con las disposiciones legales de sus respectivos países y el Ordenatario Jurídico Internacional. - Recordad que el uso de cracks para temas mas allá del simple hecho de probar un programa (POR MÁXIMO 24 HORAS) con mas posibilidades de las que ofrece el shareware, esta penalizado por la ley.

- Los MP3, películas y demás material con posible (C) que podáis bajaros a traves de los links que hayan en estas paginas también tienen que ser borrados a las 24 horas, o bien adquirir el titulo original.

- Nos reservamos el derecho de vetar la entrada a cualquier sujeto a nuestra web-site y a su vez se reserva el derecho de prohibir el uso de cualquier programa y/o información, en concordancia con los derechos de autor otorgados por el artículo 14 LPI.

- Esta web contiene material considerado para adultos asi como enlaces a webs de sexo por lo que si eres menor de edad en tu pais debes retirarte.

- Contenido: peliculas descargar peliculas cvcd CVD descargar Peliculas mp3 kazaa descargar programas download DivX music games juegos Free sex porn)

Del comentario relativo a qué naturaleza jurídica tiene una web

NATURALEZA JURÍDICA DE LA PÁGINA WEB

Esta es la primera cuestión a tener en cuenta para proteger adecuadamente una página web. Con la entrada de las Nuevas Tecnologías y la creación de la llamada Sociedad de la Información, se ha perfilado un nuevo concepto para catalogar a las obras, el término "multimedia".

Según el informe Sirinelli, que data de 1994, la palabra "multimedia" fue utilizada por primera vez, a comienzos de la década de los ochenta y con ocasión de los debates sobre el monopolio público de la televisión, para designar empresas que, viniendo del mundo de la prensa, de la edición o de la publicidad, se introducían en el audiovisual, convirtiéndose en empresas "multimedia".

El término "multimedia" es impreciso porque en las obras caracterizadas como tal, el medio es uno y no múltiple, a pesar de que puedan ser múltiples las obras integradas en la multimedia resultante.

Así, en este mismo sentido, Bercovitz entiende que las obras "multimedia" son obras con partes literarias, gráficas, musicales o de otro tipo, integradas en un mismo soporte electrónico, que refuerza la unidad de la obra resultante y facilita su almacenamiento, transmisión y difusión. No obstante, y a pesar de la conceptuación de la obra multimedia, es posible entender como tal a una única obra en un soporte multimedia, por ejemplo, una obra musical o bases de datos no protegibles específicamente por la vía del derecho de autor.

La producción multimedia es el soporte en el que ha sido almacenado, en lenguaje digital y en número no inferior a dos de diverso género, texto, sonidos, imágenes fijas y en movimiento, que pueden constituir la expresión de obras literarias, musicales, "visuales" (de las artes plásticas y fotográficas) y audiovisuales, preexistentes o creadas para su explotación a partir de tales soportes, cuya estructura y acceso están gobernados por un programa de ordenador que permite la interactividad respecto de esos elementos

¿Las producciones multimedia pueden ser obras, según el concepto dado por la Ley de Propiedad Intelectual?. Para que sean obras es necesario que el complejo de elementos de *su contenido constituya unitariamente una concreta exteriorización formal de la creación intelectual de una persona o grupo de personas dotada de originalidad.*

La originalidad se entiende en el hecho de que esa creación se individualice en virtud de una concepción personal de su creador o creadores. Esta originalidad deberá apreciarse tanto en los elementos que integran ese complejo y en el plan de acceso y recorrido no secuencial (a través de ellos), como en la estructura del conjunto de dichos elementos (excluido el programa), cuando se trate de obras preexistentes.

Llegado a este punto, es indudable que las producciones de multimedia, por lo general, son obras protegidas por el derecho de autor.

Nos parece interesante dejar claro la diferencia entre continente y contenido, es decir, que la obra multimedia parece ser cosa distinta de los programas de ordenador

que se utilicen para confeccionarla; cosa distinta del soporte es que la obra se plasme, teniendo presente el artículo 10.1ª) del Texto Refundido de la Propiedad Intelectual (en adelante, TRLPI) que refiriéndose a las obras del espíritu, habla de "creaciones originales (...) expresadas por cualquier medio, tangible o intangible, actualmente conocido o que se invente en el futuro".

La naturaleza jurídica de la Web

El diferente tratamiento jurídico que el Texto Refundido de la Ley de Propiedad Intelectual (TRLPI) dedica a cada categoría de obra intelectual exige precisiones.

· Web site como obra colectiva. Normalmente, exceptuando el creado por un autor individual, que no conlleva problemas al determinar la autoría, en el desarrollo y creación del web site intervienen diversos autores que aportan cada uno de ellos un elemento creativo a la obra final, "sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra" (art. 8 TRLPI).

En la mayoría de los supuestos, será la empresa o el productor, el titular originario de los derechos patrimoniales de propiedad intelectual, pues es quien edita y divulga la obra y, salvo pacto en contrario, así es como ha de interpretarse (art. 8.2 TRLPI).

· Web site como programa de ordenador. Una importante corriente doctrinal considera que la obra multimedia es un programa de ordenador sobre la base del artículo 91 TRLPI: "A los efectos de esta Ley, se entenderá programa de ordenador 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".

Un programa de ordenador es una secuencia de instrucciones e indicaciones utilizadas en un sistema informático para realizar una función. El régimen jurídico que se aplicaría a la web sería el de los programas de ordenador y su autoría se atribuiría a la empresa.

Esta tesis carece de base sólida porque, si bien el programa de ordenador da soporte a la página web, ésta no es sólo software sino que está compuesta por otros elementos.

· Web site como obra audiovisual. Según el artículo 86 TRLPI: "Las disposiciones contenidas en el presente Título serán de aplicación a las obras cinematográficas y audiovisuales, entendiendo por tales las creaciones expresadas mediante una serie de imágenes asociadas, con o sin sonorización incorporada, que estén destinadas esencialmente a ser mostradas a través de aparatos de proyección o por cualquier otro medio de comunicación pública de la imagen y del sonido, con independencia de la naturaleza de los soportes materiales de dichas obras".

El art. 120.1 del TRLPI, al dar la definición de grabaciones audiovisuales, habla de "fijaciones de un plano o secuencia de imágenes". Planos y secuencias son términos propios del lenguaje cinematográfico (hoy audiovisual).

Si analizamos elemento a elemento de los que componen la definición de obra audiovisual, con relación a la obra multimedia, el único conflictivo que pone en duda su asimilación es el concepto de imagen asociada. ¿Significa que, necesariamente, tiene que ser una sucesión de fotogramas con un hilo argumental?. Si así fuera, la obra audiovisual sería una obra cinematográfica y habría que argumentar por qué la

definición del artículo 86 se refiere tan sólo a la audiovisual, distinguiéndola de la cinematográfica.

· Web site como colección o base de datos. Son objeto de protección por la Ley de Propiedad Intelectual (art.12) "las colecciones de obras ajenas, de datos, o de otros elementos independientes como las antologías y bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales(...)". Lo importante es la estructura, el esfuerzo que realiza la persona que crea la base de datos para sistematizarlo porque no es original.

Esta acepción sólo puede dar lugar a derechos de autor o, y de acuerdo con la Directiva 96/9/CE, de 11 de marzo de 1996, a derechos "sui generis".

Un web site, sin duda, puede calificarse como obra multimedia, en el sentido de ser una obra única y autónoma compuesta de elementos diversos que, tradicionalmente, formaban una categoría de obra concreta. La enumeración del artículo 10 TRLPI deja de ser efectiva cuando se trata de una conjunción de audio, imagen, sonido, software, bases de datos...

La corriente doctrinal mayoritaria defiende la concepción de la página web como obra multimedia que incorpora un elemento nuevo: la interactividad, es decir, un diálogo entre el usuario y el ordenador en el que las obras se encuentran reproducidas en representación digital, tanto a efectos de la mera recuperación de ellas como de su manipulación o utilización en operaciones que pueden tener carácter creativo.

Después de lo dicho, no es dudoso que la obra multimedia no esté definida en la Ley como una categoría de obra puesto que la multimedia puede ser considerada, dependiendo de su contenido, como obra colectiva (literarias o fotográfica), bases de datos (colecciones) y obra audiovisual.

Pero no hay que olvidar que como obra debe estar protegida por el derecho de autor aunque no esté creada como concepto jurídico.

Esta complejidad respecto a su naturaleza jurídica plantea problemas respecto a cual debe ser el régimen jurídico de la página web. Una opción sería, acudir al Derecho Civil y a los contratos atípicos, estableciendo la protección de la web según la naturaleza jurídica del elemento predominante, por ejemplo, si la web contiene una base de datos, proteger la misma mediante el derecho "sui generis" y el artículo 12 del TRLPI.

No obstante, analizaremos más profundamente la protección que, hoy en día, se establece para la página web.

Inmaculada García Pérez
Especialista en Derecho Nuevas Tecnologías
14 de Febrero de 2002

Comentario relativo al Linking

http://www.infonomia.com/tematiques/index.asp?idm=1&idrev=20&num=23
Linking

¿Es la creación de *links* o enlaces con otras páginas web la esencia de Internet o es una práctica que nos puede provocar problemas legales? ¿Podemos incluir libremente en nuestra página web enlaces a otras páginas?

Para una amplia mayoría de profesionales y estudiosos de todas las disciplinas imaginables, la posibilidad de incluir en una página web referencias o enlaces a otras páginas web constituye la esencia misma de Internet. El hipertexto y los *links* permiten saltar de una página a otra y poner a nuestra disposición información relacionada con la página que estamos consultando. Pero el uso de *links* no siempre está exento de problemas legales. Técnicamente hablando, la inclusión de enlaces puede hacerse de diversas formas: estableciendo un *link* o enlace en una cadena alfanumérica determinada (por ejemplo, un nombre o una URL del tipo http://www.infonomia.com, apareciendo en ambos casos subrayada la cadena en cuestión) o estableciendo un enlace "oculto" sobre una imagen. En este último caso, al situar el ratón sobre la imagen nos aparecerá en el navegador la dirección de Internet asociada a dicha imagen, y, pulsando con el ratón, el propio navegador nos abrirá el enlace asociado a la imagen (nos llevará a la página de destino).

Este sistema de referencia tan útil ha dado pie a una serie de conflictos legales de cierta importancia, algunos de los cuales terminaron en contiendas judiciales, especialmente en Estados Unidos (para variar). Aunque la mayoría de ellos fueron resueltos, las principales cuestiones suscitadas siguen abiertas, bien porque los pleitos terminaron con un acuerdo extrajudicial, bien porque la cuestión jurídica subyacente no ha sido definitivamente resuelta. En todo caso, es importante retener que la esencia de la mayoría de conflictos sigue sin resolverse y que no siempre la solución norteamericana puede ser aplicada en otros ordenamientos (las tradiciones jurídicas respecto a la propiedad intelectual e industrial son bien distintas en sistemas anglosajones y latinos).

Los problemas más habituales que el uso de *links* ha suscitado tienen que ver con si existe libertad para incluir enlaces en una página web, si debemos establecer algún límite a esa libertad ("Deep Linking", ver http://www.infonomia.com/tematiques/index.asp?idm=1&idrev=20&num=3), y los problemas relacionados con la propiedad intelectual (las creaciones humanas en sentido amplio) y la propiedad industrial (las marcas). También han aparecido otra clase de conflictos relacionados con el *linking* y que tienen que ver con: 1) la difamación, las injurias o calumnias de terceros; 2) casos de competencia desleal; 3) casos de publicidad engañosa o no ajustada a la Ley, y 4) casos relacionados con la vulneración de la privacidad de las personas.

Algunos sitios web, simple y llanamente, prohíben la inclusión de cualquier enlace a sus páginas (ver http://www.colacao.es/legal.htm, por ejemplo, que literalmente avisa de que "queda prohibido establecer un enlace con, o un contenido de correo desde cualquier URL hasta el Web del Club Cola Cao (http://www.colacao.es) sin el expreso permiso escrito de Nutrexpa"). Este tipo de afirmaciones, aun y comprendiendo los legítimos motivos que encierran, parecen maximalistas y poco efectivas en un entorno como el de Internet, en el que la empresa o individuo que tiene una página web decide libremente qué páginas deja abiertas y accesibles a los usuarios, otorgando a tales páginas un carácter tan público como pueda tener su dirección postal. Y ello si tener en consideración otro tipo de derechos como el de cita, por ejemplo, amparados en las leyes en vigor en una amplia mayoría de estados.

Otros importantes sitios web reconocen directamente la esencia misma de Internet y se unen a la tendencia imperante en el pensamiento jurídico a nivel mundial de que los enlaces textuales son absolutamente libres (el que no quiera que su página se cite, que no la "cuelgue" ni la haga accesible al público en general), mientras que exigen ciertas normas para los enlaces relacionados con marcas registradas o logotipos. En este sentido, puede consultarse http://www.gateway.com/about/legal/logo.shtml, donde se establecen directrices para el uso de la imagen gráfica de Gateway, el segundo vendedor mundial de ordenadores vía *on-line*, o bien en el web de Nutricise Corp., http://www.nutricise.com (donde podemos leer literalmente lo siguiente: "You do not need to request permission to create a purely textual link from your site to Nutricise. However, if you'd like to use a graphic in connection with your link, you must use one of the Nutricise-approved logos below, and you must email the URL where the link will reside, indicating the particular logo you will be using"). En ambos casos, las limitaciones vienen fundamentadas en el uso restringido y lógico de logotipos e imágenes gráficas protegidas por los sistemas de propiedad industrial e intelectual.

De hecho, una parte significativa de los conflictos legales que acabaron en los tribunales norteamericanos terminaron con acuerdos extrajudiciales que acogen esa tesis de la libertad de los enlaces textuales y las limitaciones de los enlaces gráficos. Citaremos como ejemplos el del fan de las tiras cómicas de Dilbert, que tenía la llamada "The Dilbert Hack Page", en la que antes incluía –mediante un procedimiento llamado "inlining"- las tiras originales en su propio web y ahora incluye enlaces textuales al web "oficial", o al web de TotalNEWS, que incluye enlaces textuales hacia la CNN, USA Today y otros, aunque en el pasado, y mediante técnicas como el "framing", reproducía webs de terceros en su propio web.

Linking, *deep linking*, *framing*, *inlining*, metabuscadores... La sopa de términos y la constelación de posibles problemas legales parece no tener fin. Solamente un consejo: hagamos lo que hagamos, actuemos con sentido común, prudencia y respeto al esfuerzo creativo o empresarial de terceros hasta que haya normas que nos indiquen claramente qué se puede hacer y qué no. Aunque, ahora que lo pienso, estas normas deberán ser universales para que tengan alguna efectividad. Vaya problema.

j.blasco@e-LegallBCN.com

Cuestionario sobre propiedad intelectual

Extractos de la ley:

observa la idea de "divulgación" y la "publicación" (art. 4), piensa casos posibles de ello en internet.

Quién es considerado autor.

Cuál es el concepto basico de una obra original (art. 10).

Lee el artículo 10 y reflexiona sobre la posibilidad de considerar "obra" a una página web.

Cómo están protegidas las bases de datos (art. 12). ¿La protección alcanza a los contenidos, eso es, los "datos" de la base? (Ver artículos 133 y ss.)

Observa el art. 12.3, hasta dónde llega la protección de una base de datos, se te ocurre algún ejemplo?

Observa el contenido de los derechos morales de autor y ..:

Crees que el aviso legal de una página web puede decir cómo puede accederse a ella, linkearse, etc. Relacionas esto con el derecho moral de autor?

Un artículo difundido en la red se retira, pero se han hecho copias en otros servidores o buscadores, puede exigirse también su retirada??

Observa qué es el derecho de explotación (art. 17)

Qué derechos incluye el derecho de explotación (arts. 17 y ss.)

Pon un ejemplo de distribución.

La „Comunicación pública", consideras que se da esta figura al difundir contenidos o fotografías en internet.

Pon un ejemplo de Transformación e indica qué juego de derechos se da (art. 21).

Crees que se posible ceder el derecho de transformación, pero no el derecho de comunicación pública (art. 23).

En rigor, cuál es el motivo de la existencia del canon, esto es, de la compensación equitativa (art. 25). ¿Pagar el canon da permiso para difundir la copia privada?

¿Qué Orden fija los equipos sujetos al pago del canon?

Cuánto duran los derechos de autor, en general.

¿Se te ocurre algún supuesto donde se aplique el artículo 31? Piensa, por ejemplo, en la transmisión de datos por un operador de telecomunicaciones (Ono, Telefónica, etc.). ¿Crees aplicable también este precepto a Google?

Excepciones de autorización del autor

Copia privada: lee el artículo 31. 2 y luego observa las condiciones de acceso de una web de acceso a conenidos p2p (ver apartado posterior sobre cláusulas tipicas de estas webs), respecto de la copia privada. ¿Crees que se cumple con la excepción de este artículo 31.2 por ser copia privada?

Soy la editorial B: ¿Puedo comercializar un libro en Braille publicado por la editorial A?

A la vista de la naturaleza de estos contenidos docentes distribuidos en OCW, es decir, en abierto para cualquiera, ¿crees que es aplicable la excepción de enseñanza del artículo 32?

A la vista del artículo 32:

- ¿crees que es posible que un periódico digital indique que no quiere que nadie ponga enlaces a su web?

-A la vista del artículo 33, crees que si han colgado en la web de un periódico una imagen de interés (por ejemplo, el accidente de un avión) ¿ puedo utilizarla en mi web?

A la vista del artículo 37 crees que es posible acceder al contenido completo de un libro en soporte electrónico si te facilita dicho acceso la biblioteca.

¿Crees aplicable a Google books la excepción del artículo 37?

Fija tu atención al artículo 40 bis y haz una relectura, por ejemplo, de la excepción de copia privada.

¿Son transmisibles los derechos morales? (Art. 43) .

Programas de ordenador.

Cómo se definen (art. 96).

A la vista del artículo 96 pon dos ejemplos de lo que sí que está protegido y dos ejemplos de lo que no está protegido por la propiedad intelectual.

¿Crees que en estos materiales docentes se puede predicar alguna exepción del artículo 135?

En principio, qué acción inicial procede para proteger la propiedad intelectual, qué medidas se pueden solicitar.

¿A la vista del artículo 140, cuál crees que sería –aproximadamente- la indemnización que correspondería pagar a una persona que se ha descargado en internet una película recién estrenada en DVD?

Cláusulas típicas de exención en sitios más que dudosamente lícitos por la propiedad intelectual

Tras observar las normas de propiedad intelectual, qué opinión te merecen esas cláusulas?

Protección de webs

***Del comentario relativo a la protección de la página web*

15-¿Es obligatorio registrarse en el Registro de la Propiedad Intelectual para gozar de la protección de derechos de autor, por ejemplo de una página web?

16-Para qué sirve básicamente el registro en el Registro de la Propiedad Intelectual

17- Qué mecanismos de reacción básicos hay antes de llegar a los tribunales relativos a la materia.

***Del comentario relativo a qué naturaleza jurídica tiene una web*

18- ¿Qué significa "multimedia" para Bercovitz?

19- Qué es lo básico para considerar "obra" objeto de protección a las producciones multimedia.

20- Cómo se define "obra del espíritu" en el artículo 10.1ª) del Texto Refundido de la Propiedad Intelectual

21- Sobre qué base legal (artículo) algunos consideran un sitio web como un programa de ordenador a efectos de su protección.

22- Qué considera el autor del artículo sobre esa tesis.

23- Sobre qué base legal (artículo) algunos consideran un sitio web como obra audiovisual a efectos de su protección.

24- Sobre qué base legal (artículo) algunos consideran un sitio web como colección o base de datos a efectos de su protección.

25- Qué sostiene la corriente doctrinal mayoritaria sobre la concepción de una página web.

X. PRIVACIDAD Y PROTECCIÓN DE DATOS (I) GENERAL

1. Constitución y Convenio Europeo

Artículo 18

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Artículo 20

1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.

3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.

4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

Convenio Para La Protección De Los Derechos Y De Las Libertades Fundamentales, Hecho En Roma El 4 De Noviembre De 1950

Artículo 8. Derecho al respeto a la vida privada y familiar.

1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Artículo 11. Libertad de expresión y de información

1.- Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2.- Se garantiza la libertad de los medios de comunicación y la libertad de información dentro del respeto del pluralismo y de la transparencia.

2. Sentencia 292/2000 del Tribunal Constitucional sobre derecho a la protección de datos personales

Lea y tenga en cuenta que se trata de una sentencia prácticamente "fundacional" y creativa de un derecho fundamental, el derecho de protección de datos. En este punto observe la diferencia para con el derecho a la intimidad y la definición y contenidos de este derecho.

En el recurso de inconstitucionalidad núm. 1463-2000, interpuesto por el Defensor del Pueblo, contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

II. Fundamentos jurídicos

1. El Defensor del Pueblo ha interpuesto el presente recurso de inconstitucionalidad contra ciertos incisos de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD, cuya Disposición final segunda les priva de la forma de Ley Orgánica) que, a su juicio, vulneran frontalmente la reserva de ley del art. 53.1 CE, el art. 18.1 y 4 CE, al no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar así como del derecho fundamental que este Tribunal ha denominado de "libertad informática" (SSTC 254/1993, de 20 de julio, 94/1998, de 4 de mayo, y 202/1999, de 8 de noviembre).

(resumen jursiprudencia precedente)

4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.

Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y

finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

5. El art. 18.4 CE fue esgrimido por primera vez en el caso de un ciudadano a quien le denegó el Gobierno Civil de Guipúzcoa información sobre los datos que sobre su persona poseía, resuelto por la STC 254/1993, de 20 de julio. Y lo dicho en esta pionera Sentencia se fue aquilatando en las posteriores, como la relativa a las normas reguladoras del número de identificación fiscal (STC 143/1994, de 9 de mayo), o la que declaró contrario a la libertad sindical (art. 28 CE), en relación con el art. 18.4 CE, el uso por una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores con ocasión de una huelga promovida por determinado sindicato, STC 11/1998, de 13 de enero (cuya doctrina ha sido reiterada en una larga serie de Sentencias de este Tribunal resolviendo idéntica cuestión, y de entre las que merece destacarse la STC 94/1998, de 4 de mayo), o, finalmente y hasta la fecha, la STC 202/1999, de 8 de noviembre, en la que, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, se apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales.

Artículo 18, punto 1º y 4º afinidades y diferencias, el derecho autónomo del 18. 4º

Primera peculiaridad del 4º frespecto del 1º

Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos

personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, 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 cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato

personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Segunda peculiaridad

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.

8. Estas conclusiones sobre el significado y el contenido el derecho a la protección de datos personales se corroboran, atendiendo al mandato del art. 10.2 CE, por lo dispuesto en los instrumentos internacionales que se refieren a dicho derecho fundamental. Como es el caso de la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales. En el ámbito europeo, del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981, del que hemos dicho en la STC 254/1993, FJ 4, que no se limita "a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11", sino que los completa "con unas garantías para las personas concernidas, que formula detalladamente su art. 8", al que han seguido diversas recomendaciones de la Asamblea del Consejo de Europa.

Por último, otro tanto ocurre en el ámbito comunitario, con la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos, así como con la Carta de Derechos Fundamentales de la Unión Europea del presente año, cuyo art. 8 reconoce este derecho, precisa su contenido y establece la necesidad de una autoridad que vele por su respeto. Pues todos estos textos internacionales coinciden en el establecimiento de un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto para su uso o cesión. Esto es, como antes se ha visto, un haz de garantías cuyo contenido hace posible el respeto de este derecho fundamental...

3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) con el reglamento RLOPD, Real Decreto 1720/2007, de 21 de diciembre

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Texto conjunto con extractos del *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal), según materias (distinto tipo de letra y cursiva***).**

LOPD

Título I. Disposiciones generales (arts.1-3)

Título II. Principios de la protección de datos. (arts.4-12)

Título III. Derechos de las personas (arts.13-19)

Título IV. Disposiciones sectoriales

Capítulo I. Ficheros de titularidad pública (arts.20-24)

Capítulo I. Ficheros de titularidad privada (arts.25-32)

Título V. Movimiento internacional de datos (arts.33-34)

Título VI. Agencia de protección de datos (arts.35-42)

Título VII. Infracciones y sanciones (arts.43-49)

Disposiciones adicionales

Ámbito, objeto y definiciones

TÍTULO I

Disposiciones generales

Artículo 1. Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del

fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

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.

Reglamento

Artículo 2. Ámbito objetivo de aplicación.

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 4. Ficheros o tratamientos excluidos.

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Ley

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) 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.

d) 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.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) 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.

h) 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.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

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

Principios de la protección de datos, información y consentimiento

TÍTULO II

Principios de la protección de datos

Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Reglamento 2008

Artículo 8. Principios relativos a la calidad de los datos.

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Ley

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

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.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. 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.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Reglamento

Sección 2.ª Deber de información al interesado

Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Ley

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

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.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

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.

Reglamento

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

(resto de este artículo en comunicación de datos art. 11 Ley)

Reglamento, sobre el consentimiento

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. Principios generales.

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. Forma de recabar el consentimiento.

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. Revocación del consentimiento.

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Datos especialmente protegidos

Ley

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. 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.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados 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.

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

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Cesión de datos, acceso por cuenta de tercero

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

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.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Reglamento

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) 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 o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 19. Supuestos especiales.

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Ley

Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Reglamento

Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al

que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Medidas de seguridad (ver Guía de seguridad de la AGPD, en "materiales")

Ley

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán 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, 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.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Reglamento

TÍTULO VIII De las medidas de seguridad en el tratamiento de datos de carácter personal

Capítulo I Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Tener en cuenta el articulado y para profundizar, ver Guía AGPD

Capítulo III Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. Funciones y obligaciones del personal.

Artículo 90. Registro de incidencias.

Artículo 91. Control de acceso.

Artículo 92. Gestión de soportes y documentos.

Artículo 93. Identificación y autenticación.

Artículo 94. Copias de respaldo y recuperación.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. Responsable de seguridad.

Artículo 96. Auditoría.
Artículo 97. Gestión de soportes y documentos.
Artículo 98. Identificación y autenticación.
Artículo 99. Control de acceso físico.
Artículo 100. Registro de incidencias.
Sección 3.ª Medidas de seguridad de nivel alto
Artículo 101. Gestión y distribución de soportes.
Artículo 102. Copias de respaldo y recuperación.
Artículo 103. Registro de accesos.
Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Capítulo IV Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. Criterios de archivo.
Artículo 107. Dispositivos de almacenamiento.
Artículo 108. Custodia de los soportes.
Artículo 109. Responsable de seguridad.
Artículo 110. Auditoría.
Sección 3.ª Medidas de seguridad de nivel alto
Artículo 111. Almacenamiento de la información.
Artículo 112. Copia o reproducción.

Artículo 113. Acceso a la documentación.
Artículo 114. Traslado de documentación.

Ley

Deber de secreto

Artículo 10. Deber de secreto.
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Comentario ley: El incumplimiento del deber de secreto puede ser constitutivo de una sanción leve, en los términos del artículo 44.2.e), o de infracción grave de acuerdo con lo previsto en el artículo 44.3.g) en virtud del cual, 'La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.'
La vulneración del deber de guardar secreto sobre los datos de carácter personal especialmente protegidos a que hacen referencia los apartados 2 y 3 del artículo 7, así como de aquellos que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas, puede ser constitutivo de una sanción muy grave en los términos del artículo 44.4.g) de la Ley Orgánica 15/1999.

Derechos de las personas (ver reglamento arts. 23 y ss.)

Elementos generales (reglamento)
Artículo 23. Carácter personalísimo.
1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.
2. Tales derechos se ejercitarán:
a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.
b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.
c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia

de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Ley
TÍTULO III
Derechos de las personas
Artículo 14. Derecho de consulta al Registro General de Protección de Datos.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. 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.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. 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.

3. 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.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Derecho de oposición y su desarrollo reglamentario

Ley

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. 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.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Reglamento

Artículo 34. Derecho de oposición.

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. Ejercicio del derecho de oposición.

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

Artículo 36. Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

Derecho de exclusión de las guías telefónicas

De conformidad con el artículo 3.j de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado.

Concretamente, en los repertorios de abonados de servicios telefónicos, ya sean impresos en papel o disponibles por otros medios (Páginas blancas, CD-ROM, etc...), aparecen el nombre y apellidos así como la dirección y, salvo que Vd. se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general. La exclusión debe hacerse efectiva, en las guías formato papel, con la siguiente edición y, en las guías electrónicas, en el plazo de 10 dias.

Frente a esta situación, y si no se quiere que los datos sean de dominio público, sería conveniente proceder a solicitar, con carácter preventivo, que se proceda gratuitamente a la exclusión total o parcial de los datos relativos a su persona que se encuentren en los repertorios telefónicos de abonados, de conformidad con lo establecido en el artículo 28 de la Ley Orgánica 15/1999 y en el artículo 67 del Reglamento por el que se desarrolla el Título III de la Ley General de

Telecomunicaciones (Real Decreto 1736/1998), porque de otro modo sus datos seguirán utilizándose legalmente sin su consentimiento.

Ficheros privados, creación, etc.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente 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 y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. Datos incluidos en las fuentes de acceso público.

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el

consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes. La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

…

Artículo 32. Códigos tipo.

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

RLOPD Creación y registro de ficheros

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización,

el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. Tratamiento de datos en distintos soportes.

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. Ficheros en los que exista más de un responsable.

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. Notificación de la modificación o supresión de ficheros.

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

TÍTULO V

Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

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

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia 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. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones.

1. Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. *Añadido por Ley 62/2003, de 30 de diciembre.* Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de la presente Ley Orgánica.

Artículo 38. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. 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. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en

lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

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.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a 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.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.

Artículo 49. Potestad de inmovilización de ficheros.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

…

4. Protección de datos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

extracto

CAPÍTULO III.

Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas.

Artículo 33. Secreto de las comunicaciones.

VER NUEVA REDACCIÓN EN COMENTARIO SOBRE NUEVA LEY 25/2007

Artículo 34. Protección de los datos de carácter personal.

Sin perjuicio de lo previsto en el apartado 6 del artículo 4 y en el segundo párrafo del artículo anterior, así como en la restante normativa específica aplicable, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en

el ejercicio de su actividad, la protección de los datos de carácter personal conforme a la legislación vigente.

Los operadores a los que se refiere el párrafo anterior deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos de carácter personal que sean exigidos por la normativa de desarrollo de esta Ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

Artículo 35. Interceptación de las comunicaciones electrónicas por los servicios técnicos. (NO REFORMADO POR LEY 25/2007)

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a. La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.

b. Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 43.2.

Artículo 36. Cifrado en las redes y servicios de comunicaciones electrónicas.

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin

coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

Artículo 38. Derechos de los consumidores y usuarios finales.[…]

3. En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a. A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago.

b. A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

c. A recibir facturas no desglosadas cuando así lo solicitasen.

d. A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

e. A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.

f. A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.

g. A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

h. A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

4. Los usuarios de los servicios de comunicaciones electrónicas que no tengan la condición de abonados tendrán asimismo los derechos reconocidos en los párrafos a, b, d y en el primer inciso del párrafo f del apartado anterior.

5. Los usuarios finales no podrán ejercer los derechos reconocidos en los párrafos d y f del apartado 3 cuando se trate de llamadas efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen reglamentariamente, en especial a través del número 112.

Del mismo modo, y por un período de tiempo limitado, los usuarios finales no podrán ejercer el derecho reconocido en el párrafo f del apartado 3 cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

Reformado: «Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

6. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

7. El Ministerio de Ciencia y Tecnología podrá introducir cláusulas de modificación de los contratos celebrados entre los operadores y los consumidores que sean personas físicas y usuarios finales, para evitar el trato abusivo a éstos.

8. Lo establecido en este artículo se entiende sin perjuicio de la aplicación de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

Derechos de abonados y usuarios de servicios de telecomunicaciones

Según dispone el art. 38.3 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los abonados y los usuarios a los servicios de telecomunicaciones, tienen los siguientes derechos:

- A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.

- A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

- A recibir facturas no desglosadas cuando así lo solicitasen (*).

- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

- A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere.

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea al usuario que le realice una llamada (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada (*).

(*) Estos derechos sólo están reconocidos por la LGT para los abonados a servicios de comunicaciones electrónicas.

Derechos de los destinatarios de servicios de comunicaciones electrónicas

Los arts. 21 y 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, conforme a la nueva redacción, dada por la disposición final primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, establecen los siguientes derechos para los destinatarios de servicios de comunicaciones electrónicas

- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Éste precepto no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

- El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el

consentimiento que hubieran prestado, y deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

- Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales (cookies), 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.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

Cuestionario sobre Privacidad y protección de datos (I)

Actividad práctica

Después de haber cumplimentado todo el cuestionario y manejado la materia, elija cinco sitios web españoles de la índole que consideres, que incluyan en su página una "política de privacidad". Señala cuáles son estas webs, extracta la misma por cuanto a los elementos que veas en común en estas "políticas" sobre un esquema. Si realizas esta actividad en formato electrónico, adjunta al cuestionario los textos de dichas 5 políticas de privacidad (corta y pega texto).

Jurisprudencia sobre protección de datos

Sentencia 292/2000

Lee el artículo 18. 4º. ¿Ves el reconocimiento de un derecho fundamental?

Observa y relata brevemente la historia y justificación de este "nuevo" derecho.

Observa la terminología empleada para hablar de este nuevo derecho.

Qué afirma el Tribunal que comparte este nuevo derecho del apartado 4º con el derecho a la intimidad del apartado 1º.

Qué finalidad afirma el Tribunal que difiere este nuevo derecho del apartado 4º con el derecho a la intimidad del apartado 1º.

Observa la importante diferencia entre el nuevo derecho de la protección de datos y la intimidad por cuanto al objeto amparado.

Observa la importante diferencia entre el nuevo derecho de la protección de datos y la intimidad por cuanto al contenido.

Observa como define el contenido del nuevo derecho el Tribunal, esto es, las facultades que comporta el derecho. Fíjate en particular en los derechos concretos ("haz de garantías") que derivan de este derecho de protección de datos.

Ley Orgánica 15/1999 y Reglamento RLOPD

en las respuestas incluya también el número de artículo o artículos en los que se basa.

¿La ley se aplica también al tratamiento no informático de datos personales?

¿Se aplica la ley a los ficheros relativos a fines exclusivamente estadísticos?

¿Se rigen por la LOPD en general los ficheros del Registro Civil?

¿Según el RLOPD, los ficheros de los trabajadores de empresa con los dátos básicos están sujetos al reglamento?

¿Según el RLOPD, los ficheros de los empresarios individuales están sujetos al reglamento?

¿Cómo se definen en la ley los datos de carácter personal? (vaya a la definición en texto de la ley)

¿Quién se considera Responsable del fichero o tratamiento? (vaya a la definición en texto de la ley)

Y ¿encargado del tratamiento? (vaya a la definición en texto de la ley)

Enumera cinco de los principios básicos de la ley

1-

2-

3-

4-

5-

Principio de calidad (art. 4)

¿Cuándo se podrán recoger datos para su tratamiento?

Si has recogido un dato para una finalidad y lo quieres usar para otra finalidad, ¿qué es lo que prohíbe la ley?

Observa la posible sanción que se menciona del art. 44. 3 f) y compárala con las obligaciones del art. 4. Crees que se sanciona todo incumplimiento del artículo 4??

Si en un fichero de morosos consta que tu no has pagado una deuda y ya la has pagado, es obligatorio que modifiquen la información, lo puedes solicitar tú, pueden sancionar al fichero de morosos por ello??

¿Crees que es importante la exigencia del artículo 4. 6º de la LOPD a la hora de organizar la información?

¿Qué requisitos fija el RLOPD (Art. 8) sobre las finalidades de los datos recogidos?

Deber de información:

Resume de qué se nos tiene que informar cuando nos pidan datos personales (Art. 5).

Qué tipo de sanción supone no haber informado en la solicitud de datos?

¿Crees que es posible informar sólo a través de internet? (sin papel) en estos casos, ¿como se puede probar el cumplimiento de la información?

Si recoges datos y has dado información, cómo puedes probar que la has dado, p¿uedes digitalizar los sistemas de prestación de la información? (RLOPD)

Tratamiento de datos personales:

¿Cuál es la definición de "consentimiento del interesado" en la ley? (vaya a la definición en texto de la ley)

El consentimiento "inequívoco" ha de ser expreso?

Cabe el consentimiento "tácito"??

Salvo excepciones previstas, Necesito el consentimiento de alguien para tratar sus datos personales?

¿Cuándo se trata de fuentes de acceso público, es necesario el consentimiento?

Qué tipo de infracción es la falta de consentimiento cuando es exigible??

¿ Qué edad se considera que requieren los menores de edad para consentir?

¿Es posible recabar datos sobre los padres de un menor?

A quién corresponde garantizar que se comprueba la edad en el acceso a dispositivos, webs, etc. donde se requiere el consentimiento y la afirmación de que no se es un menor?

Me compro una lavadora y me solicitan los datos para el servicio técnico y también, para mandarme promociones relativas a electródomésticos y música. ¿Qué se requiere para poder hacerlo legalmente? ¿Cómo se puede hacer en una web? Se te ocurre algún ejemplo? Pon un "pantallazo" de tal ejemplo.

¿Cómo se puede revocar el consentimiento para el RLOPD? ¿Cómo NO se puede exigir la revocación del consentiemiento para el RLOPD?

Datos sensibles o especialmente protegidos

¿Cuáles son los datos especialmente protegidos, usualmente denominados "sensibles?

¿Qué tipo de consentimiento se requiere respecto de estos datos?

Para las nóminas de una empresa es relevante saber si tiene incapacidad o si forma parte de un sindicato (deducciones, retenciones, etc.) afecta esto al tipo de fichero de nóminas de la empresa???

El dato de ser o no fumador, es un dato de salud??

Cesión de datos y acceso por cuenta de tercero (arts. 11 Y SS. LOPD y RLOPD)

A La vista del art. 11 y del RLOPD, responda:

¿Cuándo pueden comunicarse datos personales objeto del tratamiento a un tercero?

Elaboro una base de datos a partir de datos de un listín telefónico en internet, ¿es necesario el consentimiento del afectado para que comunique esos datos a un tercero?

¿Puede la Universitat de València utilizar los datos que recaba de alumnos en las matrículas para elaborar estadísticas? Razone su respuesta

¿Puede la Universitat de València utilizar los datos de alumnos licenciados para cederla al Ministerio de Justicia para que tales licenciados no formen parte de jurados populares? Razone su respuesta

Podemos consentir el ceder datos sin conocer para qué finalidad van a ser utilizados.

Según el RLOPD, si damos los datos a la empresa A, y es fusionada con la empresa B, ¿se produce una cesión de datos de A a B? (mira el artículo 5 LOPD)

Acceso por cuenta de terceros

¿Es necesaria la cesión o comunicación de datos para la empresa que lleva el mantenimiento informático de la empresa que accede a los datos?

¿Qué requisitos tiene el posible acceso por terceros a los datos de los que dispones?

Según el Reglamento, en qué casos es posible la subcontratción sin la autorización para ello (art. 21)

Cuándo se han de destruir los datos por el encargado del tratamiento. ¿Se te ocurre algún caso en el que no se han de destruir estos datos? ¿En todos los casos hay que destruir o es posible que se bloqueen? (art. 22)

¿Los empleados de un banco pueden acceder libremente a todos los datos que figuran en las Bases de datos del banco?

Qué ficheros han de ser de medidas de nivel medio?

Qué ficheros han de ser de medidas de nivel alto?

Es necesaria una copia de respaldo en ficheros de nivel básico.

Que garantías deben hacerse para las pruebas de bancos de datos de nivel medio.

Los ficheros de nivel medio y alto qué tipo de auditoría deben hacer?

El registro de accesos de nivel alto, qué ha de recoger y con qué garantías?

Qué contenido tiene el documento de seguridad de todo nivel (mínimos)

Medidas de seguridad (remisión a Guía Seguridad)

Observa que el artículo 9 reenvía al reglamento las medidas de seguridad.

A partir del RLOPD, quiénes son responsables de las medidas de seguridad.

Señala tres tipos de ficheros que requieran medidas de seguridad de tipo medio:

1-

2-

3-

Señala tres tipos de ficheros que requieran medidas de seguridad de tipo ALTO:

1-

2-

3-

¿Qué tipo de ficheros son los de ONO o Telefónica?

¿Un sindicato siempre tendrá ficheros de medidas de seguridad altas?

Trabajo en casa para un banco. ¿Qué tipo de medidas de seguridad debo tener en casa? (Art. 85).

Me llevo el móvil o *Blackberry* de la empresa. ¿Qué tipo de medidas de seguridad debo tener? ¿Necesito algo para sacarla de la empresa?

Sin que se pueda profundizar este curso, tenga en cuenta la importancia de las medidas de seguridad exigibles, de especial claridad, en la Guía de Seguridad de la AGPD.

Deber de secreto.

Eres responsable o encargado del tratamiento de datos, ¿qué sanciones puedes cometer si divulgas datos a los que has accedido?

Derechos de los afectados:

Puede una asociación de consumidores ejercer mis derechos de acceso, rectificación o cancelación de datos??

Para ejercer el derecho de acceso, debo acudir a la Agencia Española, o a quién??

Puede un cliente pedirme todas las veces que quiera los datos que tenga sobre él en mi empresa??

Cuándo puedo pedir que me cancelen los datos?? Siempre??

Los datos que tenían ya no eran legítimos (por ser muy antiguos y desfasados), pero los comunicaron a otras empresas. Quién debe comunicar la rectificación o cancelación de estos datos.

Pueden utilizar los datos de una guía de teléfono??

Pueden mandarme publicidad a partir de los datos de una guía de teléfono??

Derechos de usuarios de telecomunicaciones:

Art. 23 RLOPD.

¿Te pueden cobrar o utilizar algún servicio de coste adicional para ejercer los derechos de acceso, rectificación, cancelación y oposición?

Puede mi operadora de internet, por ejemplo ONO, usar los datos que tiene sobre mí para fines comerciales, cómo??

Tengo derecho a que la factura de Telefónica, Ono, etc. no detalle las llamadas, duración, etc.??

Han recabado datos para una finalidad legítima a partir de fuentes accesibles al público. ¿Cómo puedo conseguir que me excluyan de tal tratameinto? ¿Se te ocurre algún ejemplo de justificación?

Recibo publicidad, accedo a los datos que tienen sobre mí y los tienen legítimamente. ¿Puedo evitar de algún modo que me sigan remitiendo publicidad?

¿Puede un banco decidir si me da un crédito o no a partir de un tratamiento de datos de mi persona?

Notificación e inscripción de ficheros (arts 26 LOPD y RLOPD)

Debo inscribir un fichero que solamente tenga el nombre y apellidos de la persona de contacto, el administrador o gerente de la empresa

Cómo puedo inscribir ficheros?

¿Debo obligatoriamente inscribir los ficheros manuales o en papel (listados, fichas, etc.)?

¿La notificación del fichero privado a la AGPD qué debe indicar?

¿Puede un mismo fichero estar en una base de datos, en un hosting contratado, en la PDA y en varios ordenadores de la empresa, o son necesariamente ficheros diferentes?

Si hay varios titulares del fichero –responsables-, ¿quién debe comunicar a la AGPD?

Transferencias internacionales de datos

Qué países se consideran con "protección equiparable a España"???

Qué importancia tiene ello (ver art. 34 letra k)

Puede el afectado negarse a que sus datos sean transferidos a otro país?

Si es una empresa multinacional y para ejecutar el contrato necesita pasar internacionalmente los datos, necesita una autorización específica de la Agencia??

Del ejemplo de la filial en España de una empresa alemana.

Puede la empresa alemana usar los datos recogidos por su filial española?

Qué legislación se aplica a los datos transferidos legalmente a la empresa alemana (ley española o alemana)?

Agencia de protección de datos y sanciones

Qué potestades de inspección tiene la AGPD (art. 40).

Las Agencias de las Comunidades Autónomas ¿respecto de qué ficheros pueden ser competentes? (Art. 41).

(señale el precepto-s utilizado-s para dar respuesta)

La no inscripción de un fichero qué tipo de infracción puede ser según qué condiciones.

No informar debidamente al momento de recoger datos, ¿qué tipo de infracción es?

¿Qué infracción es crear un fichero para finalidades diferentes a las legítimas de la empresa o Administración?

Qué infracción es no recabar el consentieminto cuando éste es exigible?

Trabajo en un banco, accedo para ver un vecino que situación de solvencia tiene. ¿Qué tipo de infracción cometo?

¿En principio, qué infracción es cualquier falta de las medidas de seguridad?

¿Qué tipo de infracción es recoger datos de forma fraudulenta?

¿Qué tipo de infracción es faltar a los principios de la protección de datos?

Señale ahora cuánto puede suponer una infracción…

Leve… pesetas.

grave… pesetas.

Muy grave… pesetas.

¿Es posible que una infracción grave se sancione con multa leve, en qué casos?

¿Cuándo se pueden inmovilizar los ficheros por la posible comisión de una infracción?

XI. PRIVACIDAD Y PROTECCIÓN DE DATOS (II) ADMINISTRACIÓN

Regulación LOPD y Administraciones

(tenga en cuenta otros preceptos de la LOPD, a los que se hará referencia)

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

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

Artículo 21. Comunicación de datos entre Administraciones públicas.

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo *cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso*, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. *Inciso declarado inconstitucional por la Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional.*

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información *al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o* afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales *o administrativas. Incisos declarados inconstitucionales por la Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional.*

2. *Apartado declarado contrario a la Constitución y nulo según Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional*

Aproximación a protección de datos frente a la Administración

Los datos se tienen por una finalidad conocida y legítima, y su uso y tratamiento no debe desviarse de dicha finalidad. Asimismo, los datos deben ser ciertos. Para recabar datos en principio se debe informar al sujeto afectado de que hay un fichero o tratamiento de datos y cuál es la finalidad y titularidad del mismo, asimismo, quien tenga un fichero ha de garantizar su seguridad para que no se puedan conocer por terceros estos datos. Así, el que ha de prestar sus datos, una vez conoce, debe dar su consentimiento para que se traten los datos que transmite y por ende, quien da los datos podrá revocar el consentimiento prestado para su tratamiento. Se consiente la prestación de datos para un fichero y para una finalidad, por lo que si se ha de ceder los datos de un fichero, será preciso otra vez recabar el consentimiento del afectado para ello. Entre las garantías dimanantes del derecho de autodeterminación informativa se encuentran los derechos de acceso, rectificación y cancelación. Así, una persona tiene derecho a conocer qué datos se tienen sobre él, rectificarlos si son erróneos o, en su caso, solicitar que se cancele la tenencia de sus datos.

Éste es el esquema telegráfico de la protección constitucional y legal de datos, esquema que queda muy modulado cuando se trata de la Administración. No obstante, hay que decir que la sentencia 292/2000 ha limitado y mucho las particularidades que establecía la Ley de 1999 para la Administración, al declarar inconstitucionales los preceptos 21 y 24 de la ley en diversos puntos.

Pues bien, según la situación legal y constitucional actual el panorama es el siguiente:

1- *Creación del fichero por norma previa.* En primer término, a toda Administración que quiera crear, modificar o suprimir un fichero se le exige que haya una disposición general publicada oficialmente en la que se incluya la finalidad y usos del fichero, los colectivos de quienes se pretende obtener datos o tengan la obligación de suministrarlos, cómo se recogen los datos y qué tipo de datos se recogen, quiénes son los responsables del fichero y a quienes se cederán los datos (de forma acorde a la ley y la Constitución), también se ha de especificar la seguridad de los ficheros y los órganos responsables del mismo. Por último, es preciso que conste ante quién se podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Cualquier actuación de la Administración con datos que no procedan de un fichero así dispuesto previamente será nula de pleno derecho por vulneración de derechos fundamentales, en virtud del artículo 86. 1 de la Ley 30/1992.

2- *Información previa al afectado*. Para recabar los datos, la información previa al interesado no es precisa para la Administración en casos determinados, que han sido muy limitados por el Tribunal Constitucional. Así, no es preciso informar al administrado del recogimiento de datos (art. 5 y art. 24) en razón de la Defensa nacional, la seguridad pública o la persecución de infracciones penales (no en razón de la persecución de infracciones sancionatorias). Asimismo, esta información previa del recogimiento de datos no es precisa para la Administración si una ley (y no una norma inferior) expresamente lo prevé, pero no por cualquier causa, sino que la ley habrá de establecer de forma concreta su justificación en razón de las necesidades de la Administración para cumplir eficazmente sus funciones de control y verificación, por ejemplo. Tampoco es necesaria la información previa si el uso que va a hacer la Administración es de fines históricos, estadísticos o científicos o se considera por la Agencia de Protección de Datos que esta información previa exige esfuerzos desproporcionados para la Administración. (5. 5)

3- Por cuanto al *consentimiento del afectado* para dar sus datos, éste no es preciso para las Administraciones públicas si los datos se recogen para ejercer sus funciones propias en el ámbito de sus competencias (art. 6. 2). Ahora bien, si el consentimiento en general no es preciso para la recepción de datos, sí lo será, en general, para que la Administración comunique estos datos a otras administraciones o a terceros.

4- La *cesión de datos entre administraciones* sin el consentimiento del afectado sólo es posible si es para el ejercicio de las mismas competencias concretas relativas a la finalidad por la que los recabó, o cuando esta comunicación o cesión de los datos tiene únicamente fines históricos, estadísticos o científicos. También es posible la cesión si la Administración que los elabore u obtiene lo hacía con destino a otra Administración, tal y como se había publicado previamente al crear el fichero. También, con carácter general, la cesión sin consentimiento previo será posible cuando esté autorizada por la ley (y la ley justifique razonable y proporcionalmente la necesidad y alcance de que éste consentimiento previo no sea exigible), tampoco es preciso el consentimiento previo cuando se trate de datos recogidos de fuentes accesibles al público, o cuando desde la Administración su destino sea el Defensor del Pueblo o el Tribunal de Cuentas, y figuras autonómicas afines a éstas o al Ministerio Fiscal y a Jueces y Tribunales, (arts. 11 y 21). Asimismo, en el ámbito de la Administración tributaria se prevén excepciones (art. 112.4 de la Ley General Tributaria). Debe tenerse en cuenta lo que se afirma posteriormente respecto de la normativa reciente.

Por cuanto a la cesión de datos, en particular referencia a la Administración electrónica cabe recordar lo dicho respecto de los certificados telemáticos y transmisiones de datos en su reciente regulación de 2003, antes expuesta, con relación al derecho a no presentar documentación en poder de la Administración actuante.

5- Por cuanto a los *derechos de acceso, rectificación y cancelación*, hay excepciones en el caso de la Hacienda Pública, donde es posible denegar el ejercicio en razón de no obstaculizar las actuaciones administrativas para cumplir los deberes con esta Administración o durante el transcurso de inspecciones.

También es posible la limitación legal (no infralegal) de estos derechos respecto de la Administración en razón de una protección concreta y no genérica a partir de los

bienes constitucionales de protección de intereses administrativos o de terceros, la cual aun no se ha desarrollado de forma concreta.

En el caso de los ficheros policiales las posibles excepciones de la información, consentimiento y derechos de acceso, rectificación y cancelación son mayores, sin perjuicio de la remanencia de no pocas garantías constitucionales.

Hay que decir, no obstante, que hay que estar por la regulación particular de los ficheros de materias clasificadas, los de investigación de terrorismo y delincuencia organizada, los de régimen electoral, datos estadísticos, datos de calificación del personal de Fuerzas Armadas, Registro Civil y del Registro Central de penados y rebeldes, así como el uso de videocámaras por las Fuerzas y Cuerpos de Seguridad (art. 2 ley). Asimismo, se dan particularidades respecto de los . Ficheros y Registro de Población de las Administraciones públicas (Disposición adicional segunda), el tratamiento de expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social (Disposición adicional tercera).

Hay que decir, no obstante, que hay que estar por la regulación particular de los ficheros de materias clasificadas, los de investigación de terrorismo y delincuencia organizada, los de régimen electoral, datos estadísticos, datos de calificación del personal de Fuerzas Armadas, Registro Civil y del Registro Central de penados y rebeldes, así como el uso de videocámaras por las Fuerzas y Cuerpos de Seguridad (art. 2 Ley 15/1999).

Datos y Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

Ten en cuenta el artículo 11 de la LOPD

Artículo 6. Derechos de los ciudadanos.

b) A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.

Artículo 9. Transmisiones de datos entre Administraciones Públicas.

1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley.

Artículo 35. Iniciación del procedimiento por medios electrónicos.

3. Con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

Comentario:

A mi juicio, la LAE peca de exceso de garantismo al reconocer como derecho disponible por el titular la no aportación de documentos. La LAE, que no ha afrontado como debiera la cuestión de la comunicación de datos, podía haber sido algo más atrevida. De una parte, cuando se trate de órganos de una misma Administración no parece exigible el consentimiento para el acceso a los datos[65]. De otra parte, y por lo que más interesa, podía haberse seguido la vía italiana del Decreto Legislativo 196/2003 que recuerda FERNÁNDEZ SALMERÓN[66] que tan siquiera exige ni ley ni reglamento para que pueda accederse a los datos de otra administración, sino sólo que sea necesario para el cumplimiento de las funciones, al considerarse un interés público relevante. VALERO[67] también estima falta de ambición a la LAE, que hubiera sido más razonable obligar al intercambio de información a las administraciones añadiendo la garantía de informar al ciudadano sobre la información recibida y su procedencia. Considero –también con este autor y con el apoyo del artículo 35. 2º LAE y el artículo 78. 1º LRJAP- que la participación del ciudadano en el procedimiento, si es voluntaria, puede ya entenderse como una autorización suficiente a la luz del derecho a la protección de datos personales para que la Administración Pública que ha de tramitarla localice y obtenga la información necesaria para resolverla[68]. Además, y en general, el interés público en que los actos administrativos se dicten a partir de la información necesaria para asegurar en la mayor medida posible su validez y eficacia podría permitir que la ley regulara la cuestión sin partir como premisa del consentimiento del afectado. Asimismo, siguiendo al último autor referido, esta exigencia de

---

65 FERNÁNDEZ SALMERÓN, 2003: 248.

66 *Ibídem*, 250.

67 VALERO, 2007.

68 Así, el artículo 35. 2º LAE afirma expresamente que "La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos."

consentimiento no es razonable teniendo en cuenta que en muchos casos no se conocerá la identidad del mismo, en otros casos la exigencia de consentimiento habrá de serlo a todos los afectados por ese tratamiento de datos, lo cual acentúa la disfuncionalidad de la medida.

Ahora bien, más allá de estas críticas, hay que seguir la regulación de la LAE. Y lo cierto es que sobre la base de haber reconocido un derecho, es difícil interpretarlo de otra manera que no pase por el necesario consentimiento del interesado para el acceso a la información de una a otra Administración, salvo leyes específicas que lo autorizasen.

Así las cosas, puede suscitar dudas el caso de que el ciudadano aporte la información requerida y no consienta que la Administración actuante acceda a sus datos de otras administraciones. Cabe preguntarse si la Administración debe quedar atada y vinculada a la documentación e información aportada por el ciudadano o si, por el contrario puede seguir recabando la información administrativa a otros órganos o a otras administraciones aún a pesar de que el ciudadano haya preferido aportar los documentos. En razón del 78. 1º LRJAP para el caso de dudas justificadas respecto de la información aportada del interesado, la Administración podrá realizar la actividad tendente a la averiguación de los datos. Pero como punto de partida y por defecto, en razón del derecho reconocido, no podrá accederse a la información sin el consentimiento del interesado, pese a que los medios electrónicos faciliten sobremanera esta gestión de forma masiva y automatizada al tiempo que se genera el trámite electrónico.

Ejemplos de excepciones y previsiones de cesión de datos por ley

Algunas de estas excepciones:
-Ámbito tributario (Ley 58/2003, General Tributaria, art. 94.5 y 95;
art. 94
4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.
Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.
5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo

21 de la Ley Orgánica 15/1999, de 13 de diciembre (RCL 1999, 3058), de Protección de Datos de Carácter Personal.

Artículo 95. Carácter reservado de los datos con trascendencia tributaria.
1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:
a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.
b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.
c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social, así como en la obtención y disfrute de prestaciones a cargo de dicho sistema.
d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.
e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.
f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.
g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.
h) La colaboración con los jueces y tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa en la que, previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.
i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.
j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los obligados al pago.
k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados.
2. En los casos de cesión previstos en el apartado anterior, la información de carácter tributario deberá ser suministrada preferentemente mediante la utilización de medios informáticos o telemáticos. Cuando las Administraciones públicas puedan disponer de

la información por dichos medios, no podrán exigir a los interesados la aportación de certificados de la Administración tributaria en relación con dicha información.
3. La Administración tributaria adoptará las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado.
Cuantas autoridades o funcionarios tengan conocimiento de estos datos, informes o antecedentes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos citados. Con independencia de las responsabilidades penales o civiles que pudieran derivarse, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.
Cuando se aprecie la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, la Administración tributaria deducirá el tanto de culpa o remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. También podrá iniciarse directamente el oportuno procedimiento mediante querella a través del Servicio Jurídico competente.
4. Los retenedores y obligados a realizar ingresos a cuenta sólo podrán utilizar los datos, informes o antecedentes relativos a otros obligados tributarios para el correcto cumplimiento y efectiva aplicación de la obligación de realizar pagos a cuenta. Dichos datos deberán ser comunicados a la Administración tributaria en los casos previstos en la normativa propia de cada tributo.
Salvo lo dispuesto en el párrafo anterior, los referidos datos, informes o antecedentes tienen carácter reservado. Los retenedores y obligados a realizar ingresos a cuenta quedan sujetos al más estricto y completo sigilo respecto de ellos.

-Ámbito recaudación de los recursos de la Seguridad Social (Ley 52/2003, por el que se da nueva redacción al artículo 36.6 del Texto Refundido de la Ley General de Seguridad Social);
- Persecución disciplinaria de extranjeros inmigrantes (Ley Orgánica extranjería, nueva disposición adicional quinta); DISPOSICIÓN ADICIONAL QUINTA. Acceso a la información y colaboración entre Administraciones públicas.
1. En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo.
2. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquéllos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos.

-Para prescripción de fármacos (Ley 62/2003, por la que se adiciona un sexto apartado al artículo 85 de la ley 25/1990, del Medicamento, para posibilitar el tratamiento y la cesión de datos que sean consecuencia de la implantación de un sistema de receta electrónica);

-Las subvenciones públicas (Ley 38/2003, General de Subvenciones, artículo 20.3), a efectos estadísticos

Artículo 20. Información sobre la gestión de subvenciones.

1. Los sujetos contemplados en el artículo 3 de esta Ley deberán facilitar a la Intervención General de la Administración del Estado, a efectos meramente estadísticos e informativos y en aplicación del artículo 4.1.c) de la Ley 30/1992, información sobre las subvenciones por ellos gestionadas, en los términos previstos reglamentariamente, al objeto de formar una base de datos nacional, para dar cumplimiento a la exigencia de la Unión Europea, mejorar la eficacia, controlar la acumulación y concurrencia de subvenciones y facilitar la planificación, seguimiento y actuaciones de control.

2. La referida base de datos contendrá, al menos, referencia a las bases reguladoras de la subvención, convocatorias, identificación de los beneficiarios con la subvención otorgada y efectivamente percibida, resoluciones de reintegro y sanciones impuestas. Igualmente contendrá la identificación de las personas incursas en alguna de las prohibiciones contempladas en el artículo 13 de esta Ley.

3. La cesión de datos de carácter personal que, en virtud de los apartados precedentes, debe efectuarse a la Intervención General de la Administración del Estado no requerirá el consentimiento del afectado.

-Ley orgánica 4/2007, reforma de la Ley orgánica de universidades

DISPOSICIÓN ADICIONAL VIGÉSIMO PRIMERA. Protección de datos de carácter personal.

1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.

Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.

2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3.

3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.

4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.

5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores.

-Ley Orgánica 2/2006, de 3 mayo, de Educación

Disposición adicional vigesimotercera.Datos personales de los alumnos

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal, y las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas en el seno de la Conferencia Sectorial de Educación.

-Ley 59/2003, de 19 diciembre

FIRMA ELECTRÓNICA. Normas reguladoras de firma electrónica

Artículo 17. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre (RCL 1999, 3058), de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

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

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

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley General de Telecomunicaciones 2003

Disposición adicional novena.Protección de datos personales

No será preciso el consentimiento del interesado para la comunicación de datos personales necesaria para el cumplimiento de lo previsto en los artículos 7 y 38.6 de esta Ley.

Artículo 7. Registro de operadores.

Se crea, dependiente de la Comisión del Mercado de las Telecomunicaciones, el Registro de operadores. Dicho registro será de carácter público y su regulación se hará por Real Decreto. En él deberán inscribirse los datos relativos a las personas físicas o jurídicas que hayan notificado su intención de explotar redes o prestar servicios de comunicaciones electrónicas, las condiciones para desarrollar la actividad y sus modificaciones.

Art. 38. 6. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia, garantizándose, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías. A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

-Ley 26/2006, de 17 julio , Ley de mediación de seguros y reaseguros privados

Disposición adicional novena.Tratamiento de datos en caso de contrato de reaseguro

El asegurador directo podrá comunicar al reasegurador, sin consentimiento del tomador o del asegurado, los datos que sean estrictamente necesarios para la celebración del contrato de reaseguro, en los términos previstos en el artículo 77 de la Ley 50/1980, de 8 de octubre (RCL 1980, 2295; ApNDL 12928), de Contrato de Seguros.

Cuestionario sobre Administración y derecho de protección de datos

¿En qué consiste la garantía de creación del fichero por norma previa?

¿Cuándo no es preciso informar previamente al afectado?

¿Cuándo no es preciso el consentimiento del afectado.?

¿Cuándo es posible la cesión de datos entre administraciones sin consentimiento?

¿Cuáles son las excepciones en el ejercicio de los derechos de acceso, rectificación y cancelación?

Datos personales y Ley 11/2007 de administración electrónica

Recuerda la norma general para la comunicación de datos del artículo 11 LOPD.

Es necesario el consentimiento del interesado en un procedimiento administrativo para que una Administración pueda acceder a la información del interesado que se necesita para tramitar el procedimiento (art. 6 Ley 11/2006).

Crees que si el artículo 6 no lo exigiera expresamente, sería necesario el consentimiento del interesado cuando es él quién ha iniciado el procedimiento de que se trata (por ejemplo: un solicitante de una beca).

Piensa por ejemplo en el hecho de que dentro de una misma administración no parece exigible el consentimiento para la cesión o comunicación de datos (art. 11 LOPD).

Piensa por ejemplo que por esta misma Ley 11/2006, siguiendo el artículo 11 LOPD podría haberse regulado que no será necesario el consentimiento para los casos en los que, por ejemplo, el procedimiento se inicia a instancia del interesado mismo.

¿En qué situación crees que queda la administración si el administrado no consiente en que se recaben los datos que son necesarios para la tramitación del procedimiento que el mismo administrado puede haber iniciado?

Siguiendo el artículo 35, observa cómo los sistemas normalizados de solicitud –un formulario de beca, subvención, instancia, etc.- podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

Ejemplos de excepciones legales en protección de datos

Observa las diversas excepciones al consentimiento en el tratamiento o comunicación de datos en diversas leyes.

Concreta cuándo crees que no será necesario requerir el consentimiento del extranjero según la legislación reformada.

Es necesario el consentimiento del estudiante de universidad para publicar las notas?

En el caso de los prestadores de servicios de certificación, ves alguna excepción al régimen general de cesión o comunicación de datos del artículo 11 LOPD en el art. 17 de la Ley 59/2003, de 19 diciembre de firma electrónica?

A la vista de la Disposición adicional novena de la Ley General de Telecomunicaciones 2003, con relación al artículo 38. 6º de dicha ley, ¿es necesario tu propio consentimiento para que se cedan tus datos como usuario de telecomunicaciones de una operadora a una empresa de información telefónica. Recuerda también al respecto lo que es una fuente de acceso público y su interés a efectos de consentimiento.

XII. PRIVACIDAD Y PROTECCIÓN DE DATOS III. DATOS DE TRÁFICO Y CONTROL LABORAL

1. Datos de tráfico

Derechos fundamentales en juego en materia de datos de tráfico: Tribunal Constitucional y AGPD

Tenga en cuenta el matiz del Tribunal Constitucional en sentencias 70/2002 o 56/2003. Crees que los datos de tráfico de la comunicación ya finalizada están protegidos por el artículo 18. 3 del secreto de las comunicaciones o "sólo" por el derecho a la intimidad del artículo 18. 1º y, en su caso por el derecho a la protección de datos personales (art. 18. 4º).

En efecto, en una línea jurisprudencial que recordaba el Tribunal Constitucional en su Sentencia 56/2003, se ha venido afirmando que "el concepto de "secreto", que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales"; línea emprendida ya en la Sentencia 114/1984, de 29 de noviembre, que se hacía eco de la Sentencia del TEDH de 2 de agosto de 1984, caso Malone, en la que se reconoce expresamente la posibilidad de que el artículo 8 del CEDH pueda resultar violado por el empleo de un artificio técnico que, como el recuento ("comptage"), permite registrar cuáles han sido los números telefónicos marcados en un determinado aparato, aunque no el contenido de la comunicación misma.

En todo caso, debe notarse que, en su Sentencia 70/2002 precisó el Tribunal Constitucional que "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos", de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en el proceso de comunicación (precisión que también se recoge en la STC 56/2003).

Cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad. Informe 213/2004

"Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."

LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

I

..

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

…

II

…

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

…

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto de la Ley.

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. Sujetos obligados.

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. Datos objeto de conservación.

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.

ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.

ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.

ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.

ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. Obligación de conservar datos.

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo

dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

NOTA: TÉNGASE EN CUENTA EL ARTÍCULO AL QUE SE HACE REFERENCIA, EN CONCRETO:
"38. 3.º En particular, los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos:
A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnacion de la factura del servicio o para que el operador pueda exigir su pago.
A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello."

RECUÉRDESE QUE ESTA OBLIGACIÓN PESA SOBRE:
"28. Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas."

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. Período de conservación de los datos.

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un

máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

NOTA: "DICHO ARTÍCULO LOPD dice:

"Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. 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.

3. 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.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado."

Artículo 6. Normas generales sobre cesión de datos.

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará únicamente a los agentes facultados.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. Procedimiento de cesión de datos.

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. Protección y seguridad de los datos.

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. Excepciones a los derechos de acceso y cancelación.

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. Régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley.

El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

Disposición adicional única. Servicios de telefonía mediante tarjetas de prepago.

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.
La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

…

LECRIM, art. 579 y secreto de las comunicaciones

Artículo 579.
1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación le las comunicaciones postales, telegráficas o telefónicas de las personas obre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.
4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos oras desde que fue ordenada la observación.

Doctrina básica Tribunal Constitucional para requisitos intervención de las comunicaciones telefónicas

"la intervención de las comunicaciones telefónicas sólo puede considerarse constitucionalmente legítima cuando . se ejecuta con observancia del principio de proporcionalidad; es decir, cuando su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece en los casos en que se adopta para la investigación de la comisión de delitos calificables de graves y es idónea e imprescindible para la determinación de hechos relevantes para la misma (SSTC 49/1999, de 5 de abril, FJ 8; 299/2000, de 11 de diciembre, FJ 2). La comprobación de la proporcionalidad de la medida ha de efectuarse analizando las circunstancias concurrentes en el momento de su adopción (SSTC 126/2000, de 16 de mayo, FJ 8; y 299/2000, de 11 de diciembre, FJ 2)" (STC 184/2003, de 23 de octubre; FJ 9). Faltará en todo caso el carácter necesario de la intervención cuando la misma constituya "la primera medida de investigación penal, pues el juicio de necesidad, esto es, el carácter imprescindible de la medida como parte esencial del juicio de proporcionalidad, requiere ponderar la eventual existencia de medios alternativos de investigación" (STC 184/2003, FJ 9).

Intervención de las comunicaciones en la LGT

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. Secreto de las comunicaciones.

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del

Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que

intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

2. Empleo y control laboral del correo electrónico

Grupo del artículo 29, recomendaciones

Grupo de Trabajo creado como órgano consultivo de la Unión Europea en materia de protección de datos y vida privada. Dicho Grupo, publicó en fecha 29 de mayo de 2002 un Documento proporcionando orientación sobre el contenido mínimo de las

directrices de las empresas en relación con la utilización del correo electrónico e Internet.

El documento de trabajo indica que para que una actividad de control empresarial sea legal y se justifique, deben respetarse una serie de principios:

a) Necesidad. Según este principio, el empleador, antes de proceder a este tipo de actividad, debe comprobar si una forma cualquiera de vigilancia es absolutamente necesaria para un objetivo específico. Debería plantearse la posibilidad de utilizar métodos tradicionales de supervisión, que implican una intromisión menor en la vida privada de los trabajadores, y, cuando proceda, aplicarlos antes de recurrir a una forma de vigilancia de las comunicaciones electrónicas.

b) Finalidad. Este principio significa que los datos deben recogerse con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines. En el presente contexto, el principio de «compatibilidad» significa, por ejemplo, que si el tratamiento de los datos se justifica a efectos de seguridad del sistema, estos datos no podrán tratarse posteriormente con otro objetivo, por ejemplo, para supervisar el comportamiento del trabajador.

c) Transparencia. Este principio significa que un empleador debe indicar de forma clara y abierta sus actividades. Dicho de otro modo, el control secreto del correo electrónico por el empleador está prohibido, excepto en los casos en que exista en el Estado miembro una ley que lo autorice. Ello puede ocurrir cuando se detecte una actividad delictiva particular (que haga necesaria la obtención de pruebas, y siempre que se cumplan las normas jurídicas y procesales de los Estados miembros) o cuando existan leyes nacionales que autoricen al empleador, previendo las garantías necesarias, a adoptar algunas medidas para detectar infracciones en el lugar de trabajo.

d) Legitimidad. Este principio significa que una operación de tratamiento de datos sólo puede efectuarse si su finalidad es legítima según lo dispuesto en el artículo 7 de la Directiva y la legislación nacional de transposición. La letra f) del artículo 7 de la Directiva se aplica especialmente a este principio, dado que, para autorizarse en virtud de la Directiva 95/46/CE, el tratamiento de los datos de un trabajador debe ser necesario para la satisfacción del interés legítimo perseguido por el empleador y no perjudicar los derechos fundamentales de los trabajadores. La necesidad del empleador de proteger su empresa de amenazas importantes, por ejemplo para evitar la transmisión de información confidencial a un competidor, puede considerarse un interés legítimo.

e) Proporcionalidad. Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa. El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el

objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua).

f) Exactitud y conservación de los datos. Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios) 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 empleadores deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales. Normalmente, es difícil imaginar que pueda justificarse un período de conservación superior a tres meses.

g) Seguridad. Este principio obliga al empleador 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 empleador 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 "Artículo 29" opina que las comunicaciones electrónicas que proceden de locales profesionales pueden estar cubiertas por los conceptos de «vida privada» y de «correspondencia» según lo dispuesto en el apartado 1 del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, que establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". En este sentido, el Grupo de Trabajo señala que cuando el trabajador recibe una cuenta de correo electrónico para uso estrictamente personal o puede acceder a una cuenta de correo web, la apertura por el empleador de los mensajes electrónicos de esta cuenta sólo podrá justificarse en circunstancias muy limitadas y no podrá justificarse en circunstancias normales ya que acceder a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador, debiendo prevalecer por el contrario el derecho fundamental al secreto de correspondencia.

Sentencia unificación de doctrina, control por el empresario del uso de internet y el correo electrónico del trabajador

Estatuto de los Trabajadores
Artículo 18. Inviolabilidad de la persona del trabajador.
Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo.
En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su

ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

STS, Sala ***de lo Social, de 26 de septiembre de 2007 Recurso Num.: /*966/2006, *casación de sentencia del*** T.S.J.GALICIA SOCIAL, ***Ponente*** Aurelio Desdentado Bonete

Despido disciplinario por uso incorrecto de ordenador. Contradicción en cuanto a las garantías aplicables al control por parte de la empresa de ese uso. No se aplica el régimen del artículo 18 del Estatuto de los Trabajadores, pero la empresa debe determinar previamente que el uso está controlado.

hechos probados: … El actor prestaba sus servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso, y conectado a la red de la empresa, que a su vez dispone de ADSL. El ordenador tiene antivirus propio. ----3º.- El día 11 de mayo pasado, un técnico de la empresa SOFT HARD EQUIPOS Y PROGRAMACION S.L. fue requerido para comprobar los fallos en un ordenador que la empresa señaló como del actor, comprobación, que según dicho técnico, D. Alejandro San Millán Padrón se llevó a cabo a las cinco de la tarde del citado día. En dicha comprobación se constató la existencia de virus informáticos, como consecuencia de la navegación por páginas poco seguras de internet. A presencia del Administrador de la empresa comprueba la existencia en la carpeta de archivos temporales de antiguos accesos a páginas pornográficas, que procede a almacenar en un dispositivo USB y a su impresión en papel. Dichos archivos se corresponden con imágenes y videos de carácter pornográfico. El dispositivo USB es llevado a un notario para su custodia, así como la relación de páginas que en el mismo se contiene. Las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor ni de representantes sindicales ni trabajador alguno. ----4º.- El ordenador fue retirado de la empresa para su reparación y el 30 de mayo, una vez devuelto, se procede a la misma operación esta vez a presencia de dos delegados de personal, grabándose otro USB con las páginas almacenadas en el archivo temporal, y depositándole ante el notario, con el listado de paginas que se señalan. Tampoco estaba el actor presente.

…

El 18 de mayo de 2.004…se acuerda el cese y separación como Administradora Solidaria de Dº Manuela por deslealtad y riesgo ejerciendo la acción social de responsabilidad contra ella. Los motivos son la falta de preparación e idoneidad de los contratos suscritos con la actora y D. José Antonio Pardo Cuerdo, así como haberles otorgado poderes. Estos poderes fueron revocados por el Administrador Sr. Vilela en sendas escrituras de 28 de mayo y 27 de abril de 2.004.

El fallo de dicha sentencia [apelada] es del tenor literal siguiente: "Que desestimando la excepción de incompetencia de jurisdicción y estimando la demanda formulada por D. JUAN ANTONIO PARDO CUERVO declaro la improcedencia de su despido y sin opción por la indemnización para la empresa CORUÑESA DE ETIQUETAS S.L. a salvo lo dispuesto en el artículo 11.3 del Real Decreto 1382/85 la condena a abonarle la cantidad de 90.151€ en concepto de indemnización sin derecho a salarios de tramitación".

…

FUNDAMENTOS DE DERECHO

PRIMERO.- En los hechos probados de la sentencia de instancia consta que el actor, Director General de la empresa demandada, prestaba servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso y conectado a la red de la empresa que dispone de ADSL. Consta también que un técnico de una empresa de informática fue requerido el 11 de mayo para comprobar los fallos de un ordenador que "la empresa señaló como del actor". En la comprobación se detectó la existencia de virus informáticos, como consecuencia de "la navegación por páginas poco seguras de Internet". En presencia del administrador de la empresa se comprobó la existencia en la carpeta de archivos temporales de "antiguos accesos a páginas pornográficas", que se almacenaron en un dispositivo de USB, que se entregó a un notario. La sentencia precisa que "las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor, de representantes de los trabajadores ni de ningún trabajador de la empresa". El ordenador fue retirado de la empresa para su reparación y, una vez devuelto, el 30 de mayo se procedió a realizar la misma operación con la presencia de delegados de personal. La sentencia recurrida confirma la decisión de instancia que ha considerado que no es válida la prueba de la empresa porque ha sido obtenida mediante un registro de un efecto personal que no cumple las exigencias del artículo 18 del Estatuto de los Trabajadores.

…

estamos ante un problema sobre la determinación de los límites del control empresarial sobre un ámbito que, aunque vinculado al trabajo, puede afectar a la intimidad del trabajador.

SEGUNDO.- Establecida la contradicción en los términos a que se ha hecho referencia, hay que entrar en el examen de la infracción que se denuncia del artículo 18 del Estatuto de los Trabajadores en relación con el artículo 90.1 de la Ley de Procedimiento Laboral y con el artículo 18 de la Constitución. Como ya se ha anticipado, la sentencia recurrida funda su decisión en que en la obtención del medio de prueba, a partir del cual podría acreditarse la conducta imputada por la empresa para justificar el despido, no se han respetado las exigencias del artículo 18 del Estatuto de los Trabajadores, ya que: 1º) no se demuestra que fuera necesario llevar a cabo en ese momento y sin la presencia del trabajador el examen del ordenador o al menos la continuación del examen una vez que aparecieron los archivos temporales, 2º) no consta que todo el proceso de control se realizara en el lugar y en el tiempo de trabajo, pues el ordenador fue retirado para su reparación; 3º) tampoco se respetó la dignidad del trabajador al haber realizado el control sin su presencia y 4º) el control se efectuó sin la presencia de un representante de los trabajadores.

La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa. Pero el problema es más amplio, porque, en realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales (artículo 91.1 de la Ley de Procedimiento Laboral), es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución) o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohibe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. El derecho a la intimidad, según la doctrina del Tribunal Constitucional, supone "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" y ese ámbito ha de respetarse también en el marco de las relaciones laborales, en las que "es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden ser lesivas para el derecho a la intimidad" (SSTC 142/1993, 98/2000 y 186/2000). De ahí que determinadas formas de control de la prestación de trabajo pueden resultar incompatibles con ese derecho, porque aunque no se trata de un derecho absoluto y puede ceder, por tanto, ante "intereses constitucionalmente relevantes", para ello es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho. En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada "navegación" por Internet y en el acceso a determinados archivos personales del ordenador. Estos conflictos *surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador -como sucede también con las conversaciones telefónicas en la empresa- y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa.* Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste "podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales", aunque ese control debe respetar "la consideración debida" a la "dignidad" del trabajador.

TERCERO.- Estas consideraciones muestran que el artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral. El artículo 18 del Estatuto de los Trabajadores establece que "sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo", añadiendo que en la realización de estos registros "se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible". *El supuesto de hecho de la norma es completamente distinto del que se produce con el control de los medios informáticos en el trabajo.* El artículo 18 está atribuyendo al empresario un control que excede del que deriva de su posición en el contrato de trabajo y que, por tanto, queda fuera del marco del artículo 20 del Estatuto de los Trabajadores. *En los registros el empresario actúa, de forma exorbitante y excepcional*, fuera del marco contractual de los poderes que le concede el artículo 20 del Estatuto de los Trabajadores y, en realidad, como ha señalado la doctrina científica, desempeña -no sin problemas de cobertura -una función de "policía privada" o de "policía empresarial" que la ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores de la empresa. El régimen de registros del artículo 18 del Estatuto de los Trabajadores *aparece así como una excepción al régimen ordinario que regula la Ley de Enjuiciamiento Criminal (artículo 545 y siguientes).* Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. *Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "como propietario o por otro título" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen.* Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a *la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que*, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.

De ahí que los elementos que definen las garantías y los límites del artículo 18 del Estatuto de los Trabajadores, no sean aplicables al control de los medios informáticos. En primer lugar, *la necesidad del control de esos medios no tiene que justificarse por "la protección del patrimonio empresarial y de los demás trabajadores de la empresa"*, porque la legitimidad de ese control deriva del carácter de instrumento de producción del objeto sobre el que recae. *El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación.* Así, nuestra sentencia de 5 de

diciembre de 2003, sobre el *telemarketing* telefónico, aceptó la legalidad de un control empresarial consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre los trabajadores y los clientes «para corregir los defectos de técnica comercial y disponer lo necesario para ello", razonando que tal control tiene "como único objeto ...la actividad laboral del trabajador", pues el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de "telemarketing" y los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa. El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes ..), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. En realidad, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores.

En segundo lugar, la exigencia de respetar en el control la dignidad humana del trabajador no es requisito específico de los registros del artículo 18, pues esta exigencia es general para todas las formas de control empresarial, como se advierte a partir de la propia redacción del artículo 20.3 del Estatuto de los Trabajadores. En todo caso, hay que aclarar que el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad.

En tercer lugar, la exigencia de que el registro se practique en el centro de trabajo y en las horas de trabajo tiene sentido en el marco del artículo 18, que se refiere a facultades empresariales que, por su carácter excepcional, no pueden ejercitarse fuera del ámbito de la empresa. Es claro que el empresario no puede registrar al trabajador o sus efectos personales fuera del centro de trabajo y del tiempo de trabajo, pues en ese caso sus facultades de policía privada o de autotutela tendrían un alcance completamente desproporcionado. Lo mismo puede decirse del registro de la taquilla, aunque en este caso la exigencia de que se practique en horas de trabajo tiene por objeto permitir la presencia del trabajador y de sus representantes. En todo caso hay que aclarar que las exigencias de tiempo y lugar del artículo 18 del Estatuto de los Trabajadores no tienen por objeto preservar la intimidad del trabajador registrado; su función es otra: limitar una facultad empresarial excepcional y reducirla al ámbito de la empresa y del tiempo de trabajo. *Esto no sucede en el caso del control de un instrumento de trabajo del que es titular el propio empresario.*

Por último, la presencia de un representante de los trabajadores o de un trabajador de la empresa tampoco se relaciona con la protección de la intimidad del trabajador registrado; es más bien, como sucede con lo que establece el artículo 569 Ley de Enjuiciamiento Criminal para intervenciones similares, una garantía de la objetividad y de la eficacia de la prueba. Esa exigencia no puede, por tanto, aplicarse al control normal por el empresario de los medios de producción, con independencia de que para lograr que la prueba de los resultados del control sea eficaz tenga que recurrirse a la prueba testifical o pericial sobre el control mismo.

No cabe, por tanto, aplicación directa del artículo 18 del Estatuto de los Trabajadores al control del uso del ordenador por los trabajadores, ni tampoco su aplicación analógica, porque no hay ni semejanza de los supuestos, ni identidad de razón en las regulaciones (artículo 4.1 del Código Civil).

CUARTO.- El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. La primera se refiere a los límites de ese control y en esta materia el propio precepto citado remite a un ejercicio de las facultades de vigilancia y control que guarde "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos a los que ya se ha hecho referencia al examinar las sentencias del Tribunal Constitucional 98 y 186/2000. En este punto es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. ***Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.*** De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos.

La segunda precisión o matización se refiere al alcance de la protección de la intimidad, que es compatible, con el control lícito al que se ha hecho referencia. Es claro que las comunicaciones telefónicas y el correo electrónico están incluidos en este ámbito con la protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones. La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador. La aplicación de la garantía podría ser más discutible en el presente caso, pues no se trata de comunicaciones, ni de archivos personales, sino de los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet. Se trata más bien de rastros o huellas de la "navegación" en Internet y no de informaciones de carácter personal que se guardan

con carácter reservado. Pero hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa. Así lo establece la sentencia de 3 de abril de 2007 del Tribunal Europeo de Derechos Humanos cuando señala que están incluidos en la protección del artículo 8 del Convenio Europeo de derechos humanos "la información derivada del seguimiento del uso personal de Internet" y es que esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc). Tampoco es obstáculo para la protección de la intimidad el que el ordenador no tuviera clave de acceso. Este dato -unido a la localización del ordenador en un despacho sin llave- no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador, aunque ello suscite otros problema en los que en este recurso no cabe entrar sobre la dificultad de la atribución de la autoría al demandante.

QUINTO.- A partir de las consideraciones anteriores la pretensión impugnatoria debe ser desestimada, pues, de acuerdo con una reiterada doctrina de esta Sala, el recurso se da contra el fallo y no contra los fundamentos jurídicos de la sentencia recurrida y este fallo es correcto, pues la empresa no podía recoger la información obrante en los archivos temporales y utilizarla con la finalidad que lo ha hecho. Esa actuación en el presente caso ha supuesto una vulneración de su derecho a la intimidad. *En efecto, en el supuesto de que efectivamente los archivos mencionados registraran la actividad del actor, la medida adoptada por la empresa, sin previa advertencia sobre el uso y el control del ordenador, supone una lesión a su intimidad en los términos a que se ha hecho referencia en los anteriores fundamentos. Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación*, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, "se siguió con el examen del ordenador" para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada. De esta forma, no cabe entender que estemos ante lo que en el ámbito penal se califica como un "hallazgo casual" (sentencias de 20 de septiembre, 20 de noviembre y 1 de diciembre de 2.006), pues se ha ido más allá de lo que la entrada regular para la reparación justificaba.

El recurso debe, por tanto, desestimarse con las consecuencias que de ello se derivan en orden a la imposición de las costas a la empresa recurrente, con pérdida del depósito constituido para recurrir y manteniéndose el aval en garantía del cumplimiento de la condena.

Por lo expuesto, en nombre de S. M. El Rey y por la autoridad conferida por el pueblo español.

F A L L A M O S

Desestimamos el recurso de casación para la unificación de doctrina interpuesto por la empresa CORUÑESA DE ETIQUETAS S.L., contra la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Galicia, de 25 de enero de 2.006, en el recurso de suplicación nº 5844/05, interpuesto frente a la sentencia dictada el 30 de septiembre de 2.005 por el Juzgado de lo Social nº 3 de A Coruña, en los autos nº 521/05, seguidos a instancia de D. JUAN ANTONIO PARDO CUERDO contra dicha

recurrente, sobre despido. Decretamos la pérdida del depósito constituido para recurrir, manteniéndose el aval como garantía del cumplimiento de la condena. Condenamos a la empresa recurrente al abono de los honorarios del Letrado de la parte recurrida en la cuantía que, dentro de los límites legales, fijará la Sala si a ello hubiera lugar.

Correo electrónico y uso sindical: La importante sentencia del Tribunal Constitucional en el caso CCOO vs. BBVA y el uso sindical del correo electrónico del empresario

En la sentencia 281/2005, de 7 de noviembre, el Tribunal Constitucional afronta directamente la cuestión del uso sindical de los medios electrónicos y tecnológicos de la empresa.

Desde el día 2 de febrero de 1999 el sindicato CCOO enviaba por correo electrónico, desde un servidor externo (comfia.net[69]) y a través del servidor interno del grupo BBVA, mensajes de información sindical a sus afiliados y trabajadores de este banco, sin su oposición. Sin embargo, el 13 de febrero de 2000 envió nuevos mensajes que fueron rechazados por el servidor de la empresa, lo que también ocurrió en varias ocasiones más ese mes y en noviembre de 2000. Este rechazo fue motivado por la avalancha de correos masivos procedentes de la dirección comfia.net. Ante el desmesurado tamaño de las colas de espera, el grupo BBVA decidió filtrar la entrada desde aquella dirección, siendo rechazados los mensajes, con notificación al remitente. El 26 de septiembre de 2000 la empresa dictó normas de actuación para el uso racional del correo electrónico. Entre las "Prácticas a evitar" se señalaba la posibilidad de sanción por remisión de correos ajenos a la finalidades laborales[70]. Frente al Tribunal Supremo, en su sentencia 281/2005, de 7 de noviembre, el Tribunal Constitucional estima el amparo y reconoce con cierta precisión el

69 Comfia se corresponde con Federación de Servicios Financieros y Administrativos de las Comisiones Obreras.

70 Se decía: "El correo electrónico es una herramienta de productividad que el Grupo pone a disposición de sus empleados, para el desarrollo de las funciones que les tiene encomendadas. Los usos ajenos a éstos fines son por tanto considerados inapropiados y en el límite podrían configurar falta laboral. En particular la remisión a uno o varios usuarios de correos no solicitados, especialmente si esto se hace de forma masiva (actividad conocida como *spam*) es una práctica rechazable, y, dependiendo de las circunstancias que concurran, puede llegar a ser perseguible". Así las cosas, no era expresa la prohibición del uso sindical, pero sí implícita.

derecho de uso de los medios tecnológicos de los que ya dispone la empresa para la información sindical.

En la sentencia se recuerda que el contenido de la libertad sindical incluye también el de "desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponden [a los sindicatos] (por todas, SSTC 94/1995, de 19 de junio, FJ 2; 308/2000, de 18 de diciembre, FJ 6; 185/2003, de 27 de octubre, FJ 6, y 198/2004, de 15 de noviembre, FJ 5)." (FJ 3º). Como en ocasiones anteriores, se señala que "la información sindical forma parte del contenido esencial del derecho fundamental, que el sindicato puede hacerla efectiva a través de los cauces previstos en la ley y también por medio de otros que libremente adopte siempre que respete la normalidad productiva, y que el empresario tiene que asumir ciertas cargas tasadas en la ley y dirigidas a hacer efectivo el hecho sindical informativo."

Para fundamentar la sentencia, se discierne entre el contenido esencial del derecho, los derechos y facultades adicionales fijados por regulación de desarrollo[71] y los derechos de concesión unilateral del empresario[72]. La vulneración –con motivación antisindical- incluso de estos últimos derechos puede llegar a suponer una lesión de la libertad sindical.

En el caso del uso del correo electrónico, se señala que no hay obligación de base legal por lo que las empresas "no están obligadas a dotarse de esa infraestructura informática para uso sindical"[73]. Ahora

---

71 "[L]os sindicatos pueden ostentar derechos o facultades *adicionales,* atribuidos por normas legales o por convenios colectivos, que se añaden a aquel núcleo mínimo e indisponible de la libertad sindical. […] de creación infraconstitucional y deben ser ejercitados en el marco de su regulación, pudiendo ser alterados o suprimidos por la norma legal o convencional que los establece". (FJ 3º)

72 "[P]ueden también existir derechos sindicalmente caracterizados que tengan su fuente de asignación en una concesión unilateral del empresario (SSTC 132/2000, de 16 de mayo, y 269/2000, de 13 de noviembre). En estos casos, […] el empresario […] podrá suprimir las mejoras o derechos de esa naturaleza que previamente haya concedido. Pero, no exento control, puesto que voluntad empresarial […] en que no se verifique la supresión con una motivación antisindical (STC 269/2000, de 13 de noviembre, FJ 5)." (FJ 3º).

73 FJ 5º: "que la obligación del empresario de permitir la comunicación entre el sindicato y los trabajadores mediante la utilización de su sistema interno de correo electrónico no nace de una lectura actualizada de la norma legal del art. 8.2 LOLS".

bien, si la tecnología está implantada en la empresa –hecho constatable-, se centra el debate en "la facultad del empleador de impedir un uso sindical útil para la función representativa en la empresa una vez que el sistema está creado y en funcionamiento" (FJ 6º). Sobre estos términos, el Tribunal señala que la resistencia al uso de las TICs del empresario para la información sindical, necesita "justificación en razones productivas o en la legítima oposición a asumir obligaciones específicas y gravosas no impuestas al empresario" (FJ 7º). Afirma que no se pueden oponer razones de derecho de propiedad del empresario, puesto que la titularidad permanece[74]. Por ello, se consagra la carga del empresario que cuenta con medios informáticos de que los ponga a disposición de los sindicatos para su goce pacífico, sin que unilateralmente pueda privar a los sindicatos de su empleo, con posibilidad de acudir a los tribunales si lo hace[75]. En todo caso, el Tribunal fija las condiciones para ello[76]:

"Resulta claro que el derecho a contar para uso sindical con un sistema de correo electrónico a costa del empleador no encaja dentro de los límites de dicho precepto, pues sólo podría fundarse en una interpretación extensiva del derecho a un tablón de anuncios, que pasaría a considerarse como un tablón virtual. Una lectura extensiva de ese estilo no encuentra acomodo en nuestra doctrina sobre el contenido adicional de la libertad sindical, según la cual "no corresponde a este Tribunal determinar cuál es la interpretación más correcta de tal cuerpo normativo (STC 61/1989), ni resultaría constitucionalmente obligado que estando en juego una garantía legal del derecho fundamental se incline *a priori* por la interpretación aparentemente más beneficiosa para el titular de aquél, sino que basta con constatar si la interpretación llevada a cabo salvaguarda o no suficientemente el contenido del derecho fundamental" (STC 18/2001, de 29 de enero, FJ 2)."

"No cabe entender, consecuentemente, que exista una obligación legal de facilitar la transmisión de información sindical a los trabajadores, afiliados o no, a través de un sistema de correo electrónico con cargo al empleador. Las empresas, dicho en otras palabras, no están obligadas a dotarse de esa infraestructura informática para uso sindical."

74 "No pueden oponerse a esa conclusión los elementos estructurales de la definición misma del derecho a la propiedad privada. Señaladamente porque la propiedad no resulta en ningún modo desatendida por la utilización sindical de ese tipo de instrumentos empresariales, ya que su uso no la modifica. Que dicho uso no supone por sí mismo una ablación de la propiedad lo demuestra simplemente el hecho de que como consecuencia de él no pierde el empresario su titularidad de la herramienta de producción a través de la cual transmite el sindicato su información a los trabajadores." (FJ 7º).

75 "En conclusión, sobre el empresario pesa el deber de mantener al sindicato en el goce pacífico de los instrumentos aptos para su acción sindical siempre que tales medios existan, su utilización no perjudique la finalidad para la que fueron creados por la empresa y se respeten los límites y reglas de uso que a continuación

- la comunicación sindical no podrá perturbar la actividad normal de la empresa.

- Debe armonizarse el uso empresarial y sindical de la tecnología, prevaleciendo en conflicto el uso empresarial. Para ello la empresa puede regular el uso sindical del medio electrónico, sometiéndolo a límites, no absolutos.

- El uso sindical no debe no puede "ocasionar gravámenes adicionales" al empresario.

Cuestionario sobre Privacidad y protección de datos (III) comunicaciones y control laboral

Datos de tráfico y Ley de Telecomunicaciones y Ley 25/2007

incluya el número de precepto que justifique su respuesta

En virtud del artículo 35 LGT, Los servicios técnicos pueden interceptar las comunicaciones para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, qué garantías se exigen respecto de los contenidos de las comunicaciones de los que quede constancia.

¿Es posible la utilización de procedimientos de cifrado?

Puede imponerse la obligación de facilitar los algoritmos o cualquier procedimiento de cifrado utilizado

Respecto de los derechos de los usuarios

Es necesario contar con nuestro consentimiento para que puedan recabar datos de tráfico las operadoras?

---

enunciaremos, cuyo cumplimiento deberá examinarse en cada caso. En tales condiciones no puede negarse la puesta a disposición, ni puede unilateralmente privarse a los sindicatos de su empleo, debiendo acudirse al auxilio judicial si con ocasión de su utilización el sindicato llega a incurrir en excesos u ocasionar perjuicios, a fin de que aquéllos sean atajados y éstos, en su caso, compensados." (FJ 7º).

76 "Tales condiciones o restricciones son las siguientes:

a) La comunicación no podrá perturbar la actividad normal de la empresa.

b) Tratándose del empleo de un medio de comunicación electrónico, creado como herramienta de la producción, no podrá perjudicarse el uso específico empresarial preordenado para el mismo, ni pretenderse que deba prevalecer el interés de uso sindical, debiendo emplearse el instrumento de comunicación, por el contrario, de manera que permita armonizar su manejo por el sindicato y la consecución del objetivo empresarial que dio lugar a su puesta en funcionamiento, prevaleciendo esta última función en caso de conflicto. A tal efecto resultaría constitucionalmente lícito que la empresa predeterminase las condiciones de utilización para fines sindicales de las comunicaciones electrónicas, siempre que no las excluyera en términos absolutos.

c) […] la utilización del instrumento empresarial no podrá ocasionar gravámenes adicionales para el empleador, significativamente la asunción de mayores costes." (FJ 8º).

Es necesario contar con nuestro consentimiento para que puedan utilizar con fines comerciales los datos de tráfico las operadoras?

Observa los requisitos para que las operadoras puedan hacer un tratamiento de los datos de localización (por ejemplo del móvil para servicios de radiofrecuencia).

A la hora de interpretar el alcance de las letras a y d, tenga en cuenta la nueva ley 25/2007 sobre retención de datos.

Datos de tráfico

Derechos fundamentales en juego en materia de datos de tráfico: Tribunal Constitucional y AGPD

¿Según el Tribunal Constitucional, el secreto de las comunicaciones del art. 18. 3º CE protege no sólo el contenido de la comunicación, sino también quiénes han establecido la comunicación u otros datos sobre la misma?

Sobre la base de lo anterior, crees que los datos de tráfico están específicamente protegidos por el secreto de las comunicaciones del art. 18. 3º?

IP es dato personal. Atracción de la materia desde la perspectiva de la protección de datos. Tenga en cuenta que para la AEPD el número IP es un dato personal, lo que conlleva el tratamiento de la materia, también, desde el derecho a la protección de datos personales

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Exposición de motivos:

Qué Directiva transpone esta ley

Quién se considera agente facultado para disponer de los datos de tráfico? (ver también art. 6)

Los datos a retener, recogidos en el artículo 3 son los necesarios para…

Cuál es el plazo general de conservación de los datos. Será ampliable o reducible, cómo y a qué plazos?

Los incumplimientos de obligación de puesta a disposición de los agentes facultados por qué se dice que serán infracción penal?

Texto de la ley

Para qué finalidades pueden ser requeridos los datos de tráfico por los agentes facultados? (art. 1).

Tenga en cuenta que sólo se puede acceder a datos de tráfico para "delitos graves" (en general, castigados con cinco años o más de prisión o pena).

A qué datos de tráfico se aplica la ley y cuáles se excluyen (art. 1). Es posible la conservación de los contenidos de la comunicación?

Quiénes son los obligados a la conservación de los datos? (art. 2).

Fija la atención en los tipos de datos, respectivamente respecto de internet y e-mail y telefonía por internet (art. 3).

Los operadores de telecomunicaciones para qué pueden utilizar los datos a los cuya retención están obligados (art. 4 y ver 38. 3º Ley 32/2003).

A la vista del artículo 5º de esta ley y del 16. 3º de la LOPD:

Dado que la obligación al operador de telecomunicaciones "cesa", crees que sin estar obligado podrá seguir conservando datos?

Cómo se entiende la conexión del art. 5 de esta ley con el artículo 16. 3 LOPD. Crees que supone que obligatoriamente han de mantenerse los datos de tráficos hasta que prescriba la posibilidad de que se persiga una infracción de las de la LOPD, que en su caso puede llegar a tardar en prescribir 3 años (art. 47 LOPD)?

Observa que la ley no determina el tipo de "resolución judicial", por lo que no es necesario un auto, sino una providencia podría ser suficiente.

Fija la atención –y detalla- los requisitos que impone la ley a esta "resolución judicial" (art. 7):

- justificación de la medida de retención sobre qué principios

- plazo de ejecución, determinación sobre qué criterios, qué plazo "por defecto"

Qué garantías de seguridad de los datos determina la ley: dónde crees que vendrán concretadas además de en la LOPD (cuando hace referencia a la "normativa de desarrollo") (art. 8). A priori, qué tipo de medidas de seguridad crees que habrán de tener estos ficheros?

En virtud del artículo 11 de la LOPD, crees que sería obligatoria la comunicación de la cesión de los datos por el operador de telecomunicación a los agentes que pueden acceder a los datos por resolución judicial? Según esta ley, se comunicará la cesión de los datos? (art. 9).

Respecto de tarjetas prepago (disp. Ad.) es obligatorio conocer la identidad del que compre una tarjeta. Para la cesión de estos datos es necesaria la resolución judicial?

LECRIM Y LGT, interceptación de comunicaciones…

Después del análisis de la ley, tenga en cuenta en todo caso el artículo 579 LECRIM.

Crees aplicable el artículo 579 LECRIM a internet, como comunicación postal, telegráfica, telefónica??

Crees por la vía del artículo 579 y del nuevo artículo 33 de la LGT que se pueda acceder al contenido de las comunicaciones realizadas a través de internet?

A la vista de lo que afirma el Tribunal Constitucional para la medida de intervención en las comunicaciones

Para qué delitos es posible autorizar la medida de intervención de comunicaciones?

Crees que es posible que la primera medida de investigación del delito sea la solicitud de la intervención de las comunicaciones?

Observe la nueva redacción del artículo 33 de la Ley 32/2003, LGT

Estatuto de los trabajadores y Sentencia unificación de doctrina, control por el empresario del uso de internet y el correo electrónico del trabajador

Recuerda según lo anterior qué protección tiene la correspondencia ordinaria en la Ley de Enjuiciamiento Criminal?

Lee el artículo 18 ET. De su primera lectura consideras que los requisitos para el registro de taquillas y efectos deben aplicarse para el registro del ordenador de un trabajador?

Lee el artículo 20. 3º ET. Observa el límite general que tiene el empresario para el control del cumplimiento de las obligaciones del trabajador

Sentencia:

Observa los hechos enjuiciados.

Observa que las sentencias previas a ésta, según se describe, consideraron que la prueba de la empresa no era válida por obtenerse sin los requisitos del artículo 18 del Estatuto de los trabajadores.

Observa lo afirmado por el tribunal "La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa."

Observa la cuestión más general que señala el Tribunal Supremo en que consiste el caso: "n realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución) o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. "

Observa por qué "surgen" estos conflictos de derechos y poder de control empresarial.

¿Por qué el uso de los medios informáticos queda dentro del ámbito del poder de vigilancia del empresario?

¿Considera el Tribunal Supremo que se puede aplicar el artículo 18 ET para el control del uso de los medios informáticos? ¿Por qué?

Cómo considera el Tribunal Supremo el régimen de registros del artículo 18 ET?

Qué diferencia considera el Tribunal Supremo entre el control de taquillas y el control de medios informáticos? La clave de esta diferencia es la propiedad o titularidad de las taquillas o los medios informáticos?

¿Considera el Tribunal Supremo que el control de los medios informáticos tiene que ver con "la protección del patrimonio empresarial y de los demás trabajadores de la empresa"?

Qué finalidades tiene el control del uso de los medios informáticos?

Por qué el Tribunal Supremo consideró admisible el control en el tele marketing en su sentencia de 5 de diciembre de 2003?

Una vez se sitúa la cuestión en los límites del poder de control del artículo 20. 3º y no del concreto art. 18, considera el Tribunal Supremo que la no presencia del trabajador en la inspección es contraria a su dignidad?

Considera el Tribunal Supremo aplicable las garantías de que los registros se practiquen en hora de trabajo y en el centro de trabajo?

¿la presencia de un representante de los trabajadores o de un trabajador de la empresa es necesaria en un registro informático para preservar la intimidad?

Así las cosas, entiende el Tribunal Supremo que procede la aplicación analógica de las garantías del artículo 18 ET para el registro informático?

¿Qué expectativa para los trabajadores dice el Tribunal que se ha generado por una tolerancia ya tradicional?

Qué es lo que debe hacer la empresa de acuerdo con las exigencias de buena fe.

Si la empresa cumple con esos deberes, ¿podrá entenderse que si controla el uso informático habrá vulnerado "una expectativa razonable de intimidad"?

Considera el tribunal que los archivos temporales están protegidos por el derecho a la intimidad?. Qué dijo en 2007 el TEDH?

¿Para el caso concreto porqué considera el Tribunal Supremo que la prueba era inválida? ¿Qué derecho fundamental concreto estima lesionado?

¿Crees que el empresario podría haber accedido al ordenador del trabajador sólo para detección y reparación sin que ello lesionase su derecho?

Correo electrónico y uso sindical: sentencia Tribunal Constitucional

Fija la atención en los hechos.

Según la sentencia, las empresas están obligadas a dotarse de infraestructura informática para facilitar el ejercicio de los derechos sindicales?

Si ya se cuenta con tal infraestructura informática, existe la carga para el empresario de ponerlos a disposición de los sindicatos para su actividad?

Señala las tres condiciones que pone el Tribunal Constitucional para el uso sindical de los medios informáticos.

XIII. DOMINIOS

1. Dominios genéricos de nivel superior

1. FAQs dominios

FAQs

http://arbiter.wipo.int/center/faq/domains-es.html

http://ecommerce.wipo.int/domains/index-es.html

Preguntas frecuentes sobre los nombres de dominio de Internet

En esta sección se responde a las preguntas más frecuentes que se plantean al Centro de Arbitraje y Mediación de la OMPI en relación con los nombres de dominio de Internet. Para más información sobre los aspectos jurídicos que entraña la presentación de una demanda en materia de nombres de dominio o de un escrito de contestación en ese ámbito, consulten la Política y Reglamento, las Directrices para la presentación, el Baremo de tasas y la Guía.

A. Preguntas generales

¿Qué es un nombre de dominio?

Los nombres de dominio vienen a ser direcciones de Internet fáciles de recordar y suelen utilizarse para identificar sitios Web. Por ejemplo, el nombre de dominio ompi.int se utiliza para ubicar el sitio Web de la OMPI en http://www.ompi.int o el Centro de Arbitraje y Mediación de la OMPI en http://arbiter.wipo.int. Los nombres de dominio constituyen también la base de otros métodos o aplicaciones en Internet, como la transferencia de ficheros y las direcciones de correo electrónico, por ejemplo, la dirección arbiter.mail@wipo.int se deriva también del nombre de dominio wipo.int

¿Qué es el sistema de nombres de dominio (DNS)?

Por sistema de nombres de dominio se entiende, concretamente, un sistema mundial de direcciones, a saber, la forma en que los nombres de dominio se ubican y se traducen en direcciones de Protocolo de Internet y viceversa. Los nombres de dominio

como ompi.int constituyen un nombre exclusivo correspondiente a una dirección de Protocolo de Internet (un número), que viene a ser un punto físico real en Internet.

¿Qué son los gTLD?

aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel, and .travel.

Por gTLD se entienden los dominios genéricos de nivel superior. Son los dominios de nivel superior de una dirección Internet, por ejemplo: .com, .net y .org. Siete nuevos gTLD fueron seleccionados por la ICANN (Corporación de Asignación de Nombres y Números de Internet) el 16 de noviembre de 2000, a saber: .aero (para el ámbito de la aviación); .biz (para negocios y empresas); .coop (para cooperativas); .info (sin restricciones); .museum (para museos); .name (para nombres de persona); .pro (para profesionales).

Posteriormente se han incorporado un dominio lingüístico .cat (catalán, no Cataluña) así como .jobs // .mobi // .tel // .travel

¿Qué son los ccTLD?

Los ccTLD son dominios de nivel superior correspondientes a códigos de países, por ejemplo, .mx para México. La administración de esos ccTLD se lleva a cabo de forma independiente e incumbe a las autoridades de registro designadas en el plano nacional. En la base de datos de la Entidad de Asignación de Números de Internet (IANA) figuran en la actualidad 243 ccTLD. La OMPI, que cuenta con un Programa relativo a los ccTLD, ofrece un portal de bases de datos que facilita la búsqueda en línea de información relacionada con los dominios de nivel superior correspondientes a códigos de países.

B. Controversias en materia de nombres de dominio

¿Qué tipo de controversias se plantean en materia de nombres de dominio?

Aunque su objetivo es facilitar la conexión entre los usuarios, los nombres de dominio han ido adquiriendo una importancia todavía mayor como identificadores comerciales y, como tales, han entrado en ocasiones en conflicto con los identificadores comerciales que existían antes de la llegada de Internet y que son objeto de protección por medio de derechos de propiedad intelectual.

En el ámbito de nombres de dominio, las controversias se derivan en gran parte del problema de la "ciberocupación" indebida, es decir, el registro anticipado de marcas

en tanto que nombres de dominio efectuado por terceras partes. Los "ciberocupas" se aprovechan del hecho de que el sistema de registro de nombres de dominio funcione por riguroso orden de solicitud y registran nombres de marcas, personalidades y empresas con las que no tienen relación alguna. Dado que el registro de los nombres es relativamente sencillo, los "ciberocupas" pueden registrar cientos de esos nombres en tanto que nombres de dominio. En su calidad de titulares de esos registros, los "ciberocupas" suelen subastar los nombres de dominio o tratan de venderlos directamente a la compañía o a la persona interesada, a un precio muy por encima del costo de registro. También pueden conservar el registro y aprovechar la popularidad de la persona o de la empresa con la que se asocia ese nombre de dominio para atraer clientes a sus propios sitios Web.

Las controversias relativas a los siete nuevos gTLD se rigen también por la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (Política Uniforme). Por otro lado, la mayor parte de los administradores de esos nuevos registros han formulado, o están formulando políticas específicas de solución de controversias que se produzcan durante la fase "inicial" o la fase "de arranque" del respectivo dominio. En la actualidad, la OMPI se ocupa de las controversias que se producen en la fase inicial de los dominios .info y .biz. Por lo que respecta a los registros restringidos para determinados fines, se preverán procedimientos especiales para solucionar controversias en relación con el cumplimiento de las respectivas restricciones para el registro.

¿Por qué se plantean tantas controversias?

En la comunidad de Internet no hay acuerdo alguno que permita que los organismos encargados del registro de nombres de dominio lleven a cabo un examen previo para anticipar posibles nombres problemáticos. Las razones son varias, desde la voluntad de facilitar el registro en aras de la actividad empresarial, pasando por las dificultades prácticas de determinar quién es el titular de los derechos de un nombre, hasta la necesidad de tener en cuenta el principio de la libertad de expresión. Además, la importancia comercial cada vez mayor de los nombres de dominio de Internet ha generado un número creciente de casos de "ciberocupación" indebida, lo que se traduce en un mayor número de controversias y litigios entre los ocupantes y las empresas o individuos cuyos nombres han sido registrados de mala fe.

¿Por qué empezó la OMPI a ocuparse de la solución de controversias?

El auge de Internet como plataforma para los negocios y las actividades empresariales ha sido particularmente importante en el último decenio, aunque no se han elaborado normas jurídicas internacionales para solucionar las controversias en el ámbito de los nombres de dominio. Para la Corporación de Asignación de Nombres y Números de Internet (ICANN), organización encargada, entre otras cuestiones, de la gestión de los dominios genéricos de nivel superior como .com, .net y .org, era obvia la

necesidad urgente de encontrar una salida al problema de las controversias. Por otro lado, se consideró que la negociación de un nuevo tratado internacional en ese ámbito demoraría demasiado tiempo y que si se promulgaban nuevas leyes nacionales, lo más probable es que hubiera demasiadas divergencias entre unas y otras legislaciones. Lo que se precisaba eran procedimientos uniformes y vinculantes en el plano internacional para solucionar controversias en las que, con frecuencia, están implicadas partes de distintos países. Respaldada por sus Estados miembros, la OMPI, cuyo mandato es promover la protección de la propiedad intelectual en el mundo, organizó una serie de amplias consultas en el plano mundial con los miembros de los círculos de Internet, tras las cuales preparó y publicó un informe que contenía recomendaciones relacionadas con los problemas que se plantean en el ámbito de los nombres de dominio. Sobre la base de las recomendaciones que contenía ese informe, la ICANN aprobó la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio, que entró en vigor el 1 de diciembre de 1999 y cuya aplicación concierne a todas las autoridades encargadas del registro de nombres de dominio de Internet acreditadas por la ICANN. En virtud de la Política Uniforme, la OMPI es el principal proveedor de servicios de solución de controversias en materia de nombres de dominio que goza de acreditación de la ICANN. Según las estadísticas disponibles, a finales del año 2001, cerca del 60% de las demandas interpuestas en virtud de la Política Uniforme se habían presentado ante la OMPI. Por otro lado, un número cada vez mayor de autoridades de registro de dominios de nivel superior correspondientes a códigos de países optan por la OMPI en tanto que proveedor de servicios de solución de controversias.

¿Qué es la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio?

La Política Uniforme de Solución de Controversias (Política Uniforme) fue adoptada por la Corporación de Asignación de Nombres y Números de Internet (ICANN) el 26 de agosto de 1999. La Política Uniforme se formuló sobre la base de las recomendaciones contenidas en el Informe sobre el Primer Proceso de la OMPI relativo a los Nombres de Dominio de Internet, que se centraba en los problemas que plantea el conflicto entre las marcas y los nombres de dominio. Por otro lado, en ese mismo Informe se aludía a una serie de cuestiones que se consideraron que quedaban fuera del alcance del Primer Proceso de la OMPI y que se han abordado en el posterior Informe sobre el Segundo Proceso de la OMPI relativo a los Nombres de Dominio de Internet.

¿Cómo funciona la Política Uniforme?

Cuando el titular de una marca considera que el registro de un nombre de dominio constituye una infracción de su marca, puede interponer una demanda en virtud de la Política Uniforme.

En virtud de la cláusula tipo de solución de controversias que consta en las condiciones relativas al registro de un nombre en un gTLD, el titular del registro de un nombre tiene la obligación de someterse a ese procedimiento.

En virtud de la Política Uniforme, el demandante tiene la facultad de interponer una demanda ante un proveedor de servicios de solución de controversias, en la que debe especificar, ante todo, el nombre de dominio de que se trate, el demandado o titular del nombre de dominio, la autoridad ante la cual se procedió al registro y las razones en las que se basa la demanda. Entre esas razones figuran, como criterios centrales, el hecho de que el nombre de dominio sea idéntico o similar a una marca respecto de la cual el demandante tenga derechos; las razones por las cuales se considera que el demandado no tiene derechos ni intereses legítimos respecto del nombre de dominio que ha sido objeto de demanda; y las razones de que se considere que el nombre de dominio ha sido registrado y usado de mala fe.

Por otro lado, el demandado tiene la oportunidad de revocar esas acusaciones. A su vez, el proveedor de servicios (por ejemplo, el Centro de Arbitraje y Mediación de la OMPI) designa a un experto al que incumbirá decidir si es menester transferir el nombre de dominio.

¿Qué posibilidades ofrece la OMPI como proveedor de servicios de solución de controversias?

En el marco de su mecanismo de solución de controversias, la OMPI cuenta con expertos altamente cualificados e imparciales y ofrece procedimientos administrativos completos y rápidos en los que la tónica es la imparcialidad y la credibilidad. El mecanismo de solución de controversias de la OMPI es una alternativa mucho más rápida que la vía judicial tradicional. Los casos relacionados con los nombres de dominio que se presenta a la OMPI suelen resolverse en menos de dos meses, recurriendo a procedimientos en línea, a diferencia de los procedimientos ante los tribunales, que pueden ser mucho más largos. Las tasas son también mucho menores que las que se aplican en los procedimientos ante los tribunales. No se realizan vistas con asistencia de las partes, salvo en casos extraordinarios. Los requisitos mínimos de presentación que se exigen contribuyen también a reducir los costos. Para la solución de un caso relacionado con uno a cinco nombres de dominio y con intervención de un solo experto, los costos se elevan a 1.500 dólares de los EE.UU.; si intervienen tres expertos, el costo total sería de 4.000 dólares de los EE.UU. Si el caso está relacionado con seis a 10 nombres de dominio, el costo será de 2.000 dólares de los EE.UU. si sólo interviene un experto y de 5.000 dólares de los EE.UU. si intervienen tres expertos.

¿Qué soluciones ofrece la OMPI? ¿Son vinculantes sus decisiones?

Los casos relativos a los nombres de dominio se resuelven mediante la transferencia o el rechazo de la demanda, es decir, se rechaza la demanda y el demandado conserva el nombre de dominio. También es posible solicitar la cancelación del nombre de dominio.

En la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio no se prevé compensación económica ni mandamientos judiciales en las controversias relativas a los nombres de dominio. Las autoridades acreditadas de registro de nombres de dominio que hayan accedido a atenerse a la Política Uniforme deberán dar seguimiento a la resolución que se dicte tras un período de 10 días, a menos de que dicha resolución sea objeto de apelación. Las resoluciones que dictan los grupos de expertos son vinculantes en la medida en que las autoridades acreditadas de registro

tienen la obligación de tomar las medidas necesarias para dar seguimiento a la decisión adoptada, como la transferencia del nombre de dominio en cuestión. Ahora bien, en virtud de la Política Uniforme, todas las partes tienen la posibilidad de someter la controversia ante el tribunal de una jurisdicción competente a fin de que dicte una resolución independiente. En la práctica, rara vez se recurre a ese procedimiento.

¿Qué iniciativas ha tomado la OMPI además de la administración de casos en virtud de la Política Uniforme?

La Política Uniforme de Solución de Controversias en materia de Nombres de Dominio se concibió originalmente para la solución de controversias que se plantearan en los dominios genéricos de nivel superior tales como .com, .net, y .org. Sin embargo, varias autoridades de registro en los dominios de nivel superior correspondientes a códigos de países han empezado ya a aplicar la Política Uniforme o políticas similares y la propia OMPI presta ya servicios de solución de controversias en relación con los dominios de nivel superior correspondientes a códigos de países, por ejemplo, .ve para Venezuela, y .tv para Tuvalú.

Tras haber abordado cuestiones relacionadas con las marcas en el marco del Primer Proceso de la OMPI relativo a los Nombres de Dominio, en el Segundo Proceso de la OMPI relativo a los Nombres de Dominio se abordó la cuestión de la protección de otros identificadores además de las marcas, como las indicaciones geográficas, por ejemplo, para las regiones productoras de vino, los nombres de persona, los nombres comerciales, y los nombres y siglas de organizaciones internacionales intergubernamentales. En el ámbito de los nombres de dominio y de la solución de controversias a ese respecto, la evolución es constante.

C. Mecanismos de solución controversias relativas a los nombres de dominio genéricos

¿Cómo se interpone una demanda o un escrito de contestación?

A los fines de la presentación de una demanda, la mayoría de las partes consultan las Directrices de la OMPI para la presentación de demandas, y utilizan la demanda tipo y el escrito de contestación tipo de la OMPI. Las partes deben familiarizarse con la Política y el Reglamento, y con el Reglamento Adicional de la OMPI. Por otro lado, y en aras de la presentación del caso, se recomienda que las partes consulten las resoluciones de casos que se hayan dictado hasta la fecha.

¿Qué costos entraña el procedimiento y a quién incumbe el pago?

El importe que debe pagarse depende de dos criterios, a saber, el número de nombres de dominio objeto de controversia y el número de expertos (uno o tres) que intervienen en el caso. En la tasa está incluido un importe adjudicado al Centro en concepto de tasa de administración y un importe que debe pagarse al/a los experto(s). En cuanto a la cuestión de determinar a quién incumbe el pago: en caso de que sólo

intervenga un experto, el total de la tasa correrá por cuenta del demandante. Si se trata de un grupo de expertos integrado por tres miembros a petición del demandante, el total de la tasa correrá por cuenta del demandante. En los casos en los que intervengan grupos de expertos integrados por tres miembros a petición del demandado, el total de la tasa se dividirá en dos partes iguales entre el demandante y el demandado.

¿A quién incumbe tomar las decisiones y de qué forma vela la OMPI por impedir un conflicto de intereses?

La función que desempeña la OMPI en el procedimiento de solución de controversias es de índole administrativa. Facilita la comunicación entre las partes y, sobre la base de las circunstancias específicas de cada controversia (como la nacionalidad de las partes y el idioma en que tengan lugar los procedimientos) designa a un "árbitro" o experto a fin de examinar la controversia y de tomar una decisión. Los miembros de los grupos de expertos son seleccionados a partir de una lista de profesionales independientes facultados para tomar decisiones en ese tipo de casos. Una y otra parte en la controversia tienen la facultad de designar a uno o tres expertos para que se ocupen del caso. Antes de ocuparse de un caso, los expertos deben confirmar a la OMPI que no existe ningún conflicto potencial de intereses y deben hacer una declaración por escrito en la que expongan cualquier circunstancia que deba tenerse en cuenta antes de su designación.

¿Qué factores inciden en las decisiones de los expertos?

El grupo de expertos toma decisiones sobre la base de los criterios, que son acumulativos, contenidos en la Política Uniforme, que también expone ejemplos prácticos de la forma en que las partes pueden probar el cumplimiento de dichos criterios, a saber:

i) el hecho de que el nombre de dominio sea idéntico o similar al punto de crear confusión a una marca de fábrica o de servicio respecto de la cual tenga derechos el demandante;

ii) el hecho de que el demandado tenga cualquier derecho o interés legítimo respecto del nombre de dominio (por ejemplo, la oferta legítima de bienes y servicios utilizando el mismo nombre);

iii) el hecho de que el nombre de dominio haya sido registrado y se esté utilizando de mala fe.

¿Se percibe compensación por daños y perjuicios?

No. En virtud de la Política Uniforme, el experto sólo puede ordenar la transferencia o la cancelación del/de los nombre(s) de dominio o rechazar la demanda. No incumbe al grupo de expertos pronunciar laudos monetarios.

¿Se publican los casos y las resoluciones en línea?

El caso se publica en línea una vez que la OMPI ha registrado la demanda. Las resoluciones se publican en línea en cuanto las partes en la controversia hayan recibido notificación de la resolución. Se puede efectuar una suscripción para recibir mensajes electrónicos diarios en los que se notifiquen las resoluciones dictadas una vez se hagan públicas. Los mensajes electrónicos anteriores en los que se exponen resoluciones adoptadas están archivados en línea.

¿Puede buscarse información en línea en relación con los números de los casos, los nombres de dominio, las resoluciones u otros datos relativos a los casos?

Es posible efectuar búsquedas por nombre de dominio o número de caso en todos los casos administrados por la OMPI en virtud de la Política Uniforme, además de utilizar el índice consultable en línea de las resoluciones de la OMPI basadas en la Política Uniforme. Por otra parte, están disponibles los cuadros en los que figuran todos los casos tramitados ante el Centro de Arbitraje y Mediación de la OMPI y todas las decisiones dictadas por los grupos de expertos de la OMPI. Las estadísticas relativas a la tramitación de casos y a las resoluciones se actualizan diariamente.

2. La "Política" del ICANN

POLÍTICA UNIFORME DE SOLUCIÓN DE CONTROVERSIAS

EN MATERIA DE NOMBRES DE DOMINIO

Política aprobada el 26 de agosto de 1999

Documentos de ejecución aprobados el 24 de octubre de 1999

Traducción al español de la Organización Mundial de la Propiedad Intelectual

Nota: Esta política está en vigor. Consulte el sitio www.icann.org/udrp/udrp-schedule.htm para obtener información sobre el calendario de ejecución.

1. Objetivo. La presente Política uniforme de solución de controversias en materia de nombres de dominio (la "Política") ha sido aprobada por la Corporación de Asignación de Nombres y Números de Internet ("ICANN"), se incorpora mediante referencia en su acuerdo de registro y establece las cláusulas y condiciones en relación con una controversia que surja entre usted y cualquier otra parte distinta a la nuestra (el registrador) sobre el registro y utilización de un nombre de dominio de Internet registrado por usted. El procedimiento establecido en virtud del párrafo 4 de la presente Política se llevará a cabo de conformidad con el Reglamento de la Política uniforme de solución de controversias en materia de nombres de dominio (el

"Reglamento"), disponible en www.icann.org/udrp-rules-24oct99.htm, y el Reglamento Adicional del proveedor del servicio de solución de controversias administrativas seleccionado.

2. Declaraciones. Mediante el acto de solicitar el registro de un nombre de dominio o la conservación o renovación de un registro de nombre de dominio, usted declara y garantiza al registrador que a) las declaraciones que ha efectuado en su acuerdo de registro son completas y exactas; b) a su leal saber y entender, el registro del nombre de dominio no infringe ni viola de otra manera los derechos de un tercero; c) no registra el nombre de dominio con fines ilícitos y d) no utilizará a sabiendas el nombre de dominio para infringir cualquier legislación o reglamento aplicables. A usted le corresponderá determinar si su registro de nombre de dominio infringe o viola los derechos de un tercero.

3. Cancelaciones, cesiones y cambios. El registrador cancelará, cederá o efectuará cambios de otra manera en los registros de nombres de dominio habida cuenta de las siguientes circunstancias:

a.a reserva de lo previsto en el párrafo 8, una vez recibidas instrucciones que usted o su agente autorizado le envíen por escrito o por medios electrónicos adecuados a fin de que tome dichas medidas;

b. una vez recibida una orden procedente de un tribunal judicial o de arbitraje, en cada jurisdicción correspondiente, por la que se exija la adopción de dichas medidas; y/o

c.una vez recibida una resolución de un grupo administrativo de expertos por la que se exija la adopción de dichas medidas en cualquier procedimiento administrativo en el que usted sea parte y que haya sido llevado a cabo en virtud de la presente Política o de una versión posterior de la presente Política aprobada por la ICANN. (Véase el párrafo 4.i) y k).

4. Procedimiento administrativo obligatorio.

El presente párrafo establece el tipo de controversias en las que usted deberá someterse a un procedimiento administrativo obligatorio. Este procedimiento se llevará a cabo ante uno de los proveedores de servicios de solución de controversias administrativas que figuran en www.icann.org/udrp/approved-providers.htm (cada uno de ellos un "proveedor").

a. Controversias aplicables. Usted estará obligado a someterse a un procedimiento administrativo obligatorio en caso de que un tercero (un "demandante") sostenga ante el proveedor competente, en cumplimiento del Reglamento, que

i) usted posee un nombre de dominio idéntico o similar hasta el punto de crear confusión con respecto a una marca de productos o de servicios sobre la que el demandante tiene derechos; y

ii) usted no tiene derechos o intereses legítimos respecto del nombre de dominio; y

iii) usted posee un nombre de dominio que ha sido registrado y se utiliza de mala fe.

En el procedimiento administrativo, el demandante deberá probar que están presentes cada uno de estos tres elementos.

b. Pruebas del registro y utilización de mala fe. A los fines del párrafo 4.a)iii), las circunstancias siguientes, entre otras, constituirán la prueba del registro y utilización de mala fe de un nombre de dominio, en caso de que el grupo de expertos constate que se hallan presentes:

i) Circunstancias que indiquen que usted ha registrado o adquirido el nombre de dominio fundamentalmente con el fin de vender, alquilar o ceder de otra manera el registro del nombre de dominio al demandante que es el titular de la marca de productos o de servicios o a un competidor de ese demandante, por un valor cierto que supera los costos diversos documentados que están relacionados directamente con el nombre de dominio; o

ii) usted ha registrado el nombre de dominio a fin de impedir que el titular de la marca de productos o de servicios refleje la marca en un nombre de dominio correspondiente, siempre y cuando usted haya desarrollado una conducta de esa índole; o

iii) usted ha registrado el nombre de dominio fundamentalmente con el fin de perturbar la actividad comercial de un competidor; o

iv) al utilizar el nombre de dominio, usted ha intentado de manera intencionada atraer, con ánimo de lucro, usuarios de Internet a su sitio Web o a cualquier otro sitio en línea, creando la posibilidad de que exista confusión con la marca del demandante en cuanto a la fuente, patrocinio, afiliación o promoción de su sitio Web o de su sitio en línea o de un producto o servicio que figure en su sitio Web o en su sitio en línea.

c.Cómo demostrar sus derechos y sus legítimos intereses sobre el nombre de dominio al responder a una demanda. Cuando reciba una demanda, usted deberá remitirse al párrafo 5 del Reglamento al determinar la manera en que deberá preparar su escrito de contestación. Cualquiera de las circunstancias siguientes, entre otras, demostrará sus derechos o sus legítimos intereses sobre el nombre de dominio a los fines del párrafo 4.a)ii) en caso de que el grupo de expertos considere que están probadas teniendo en cuenta la evaluación que efectúe de todas las pruebas presentadas:

i) antes de haber recibido cualquier aviso de la controversia, usted ha utilizado el nombre de dominio, o ha efectuado preparativos demostrables para su utilización, o un nombre correspondiente al nombre de dominio en relación con una oferta de buena fe de productos o servicios; o

ii) usted (en calidad de particular, empresa u otra organización) ha sido conocido corrientemente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios; o

iii) usted hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera equívoca o de empañar el buen nombre de la marca de productos o de servicios en cuestión con ánimo de lucro.

d. Selección de proveedor. El demandante seleccionará al proveedor de entre los aprobados por la ICANN transmitiendo la demanda a ese proveedor. El

proveedor seleccionado administrará el procedimiento, excepto en los casos de acumulación descritos en el párrafo 4.f).

e. Inicio del procedimiento y proceso, y nombramiento del grupo administrativo de expertos. El Reglamento establece el proceso para el inicio y la realización de un procedimiento, así como para el nombramiento del grupo de expertos que resolverá la controversia (el "grupo administrativo de expertos").

f. Acumulación. En caso de existan numerosas controversias entre usted y el demandante, tanto usted como el demandante podrán solicitar la acumulación de las controversias ante un único grupo administrativo de expertos. Esta petición se efectuará al primer grupo administrativo de expertos nombrado para entender en una controversia entre las partes. Este grupo administrativo de expertos podrá acumular ante sí dichas controversias haciendo uso de sus facultades, siempre y cuando las controversias consolidadas se rijan por la presente Política o una versión posterior de la presente Política aprobada por la ICANN.

g. Tasas y honorarios. Todas las tasas que cobre un proveedor en relación con cualquier controversia ante un grupo administrativo de expertos de conformidad con la presente Política serán pagadas por el demandante, excepto en los casos en que usted elija ampliar el grupo administrativo de expertos de uno a tres miembros, tal y como prevé el párrafo 5.b)iv) del Reglamento, en cuyo caso las tasas se repartirán equitativamente entre usted y el demandante.

h. Participación del registrador en los procedimientos administrativos. El registrador no participa ni participará en la administración o realización de ningún procedimiento ante un grupo administrativo de expertos. Además, no tendrá ninguna responsabilidad como consecuencia de cualquier resolución dictada por un grupo administrativo de expertos.

i. Recursos jurídicos. Los recursos disponibles para el demandante de conformidad con cualquier procedimiento ante un grupo administrativo de expertos se limitarán a exigir la cancelación del nombre de dominio que usted posee o la cesión al demandante del registro de un nombre de dominio que usted posee.

j. Notificación y publicación. El proveedor notificará al registrador cualquier resolución adoptada por un grupo administrativo de expertos respecto de un nombre de dominio que usted haya registrado ante dicho registrador. Todas las resoluciones adoptadas en virtud de la presente Política se publicarán íntegramente en Internet, excepto cuando un grupo administrativo de expertos determine de manera excepcional que se corrijan partes de la resolución.

k. Disponibilidad de procedimientos judiciales. Los requisitos establecidos en el párrafo 4 para el procedimiento administrativo obligatorio no impedirán que usted o el demandante sometan la controversia a un tribunal competente a fin de obtener una resolución independiente antes de que se inicie dicho procedimiento o después de su conclusión. Si un grupo administrativo de expertos decide que el registro de un nombre de dominio que usted posee debe cancelarse o cederse, el registrador esperará diez (10) días hábiles (por días hábiles se entenderán los días vigentes en el lugar del domicilio de la oficina principal del registrador) tras haber sido informado por el proveedor aplicable de la resolución del grupo administrativo de expertos antes de ejecutar esa resolución. A continuación, ejecutará la resolución a no

ser que haya recibido de usted, durante ese período de diez (10) días hábiles, documentos oficiales (como la copia de una demanda, sellada por el oficial del juzgado) que indiquen que usted ha iniciado una demanda judicial contra el demandante en una jurisdicción a la que se haya sometido el demandante en virtud del párrafo 3.b)xiii) del Reglamento. (En general, esa jurisdicción será el domicilio de la oficina principal del registrador o el que figura a su nombre en la base de datos "Whois". Véanse los párrafos 1 y 3.b)xiii) del Reglamento sobre los pormenores.) Si el registrador recibe dichos documentos en un plazo de diez (10) días hábiles, no ejecutará la resolución del grupo administrativo de expertos ni adoptará ninguna medida hasta que haya recibido i) pruebas satisfactorias de que se ha producido una solución entre las partes; ii) pruebas satisfactorias de que su demanda judicial ha sido rechazada o retirada o iii) una copia de una orden dictada por dicho tribunal por la que se rechaza su demanda o se ordena que usted no tiene derecho a continuar utilizando el nombre de dominio.

5. Otro tipo de controversias y litigios. Las demás controversias entre usted y cualquier otra parte distinta a la del registrador relativas al registro de un nombre de dominio que no se realicen en virtud de las disposiciones del párrafo 4 para el procedimiento administrativo obligatorio se resolverán entre usted y dicha parte mediante una acción ante los tribunales, arbitraje u otro procedimiento que pueda estar disponible.

6. Participación del registrador en las controversias. El registrador no participará de ninguna manera en cualquier controversia que surja entre usted y otra parte distinta a la del registrador relativa al registro y utilización de su nombre de dominio. Usted no nombrará al registrador en calidad de parte ni lo incluirá de otra manera en dicho procedimiento. En caso de que el registrador sea nombrado en calidad de parte en dicho procedimiento, se reserva el derecho a formular todas las defensas que considere apropiadas y a adoptar cualquier otra medida necesaria para su defensa.

7. Mantenimiento de la condición jurídica. El registrador no cancelará, cederá, activará, desactivará o cambiará de otra manera la condición jurídica de cualquier registro de nombre de dominio en virtud de la presente Política a excepción de lo previsto en el párrafo 3.

8. Cesiones durante una controversia.

a. Cesiones de un nombre de dominio a un nuevo titular. Usted no podrá ceder su registro de nombre de dominio a otro titular i) durante un procedimiento administrativo pendiente iniciado de conformidad con el párrafo 4 o durante un período de quince (15) días hábiles (por días hábiles se entenderán los días vigentes en el lugar del domicilio social principal del registrador) a partir de la conclusión de dicho procedimiento; o ii) durante un procedimiento judicial o arbitraje pendientes iniciados en relación con su nombre de dominio a no ser que la parte a la que se ceda el registro del nombre de dominio acepte, por escrito, que la resolución del tribunal o del árbitro sea de carácter obligatorio. El registrador se reserva el derecho a cancelar cualquier cesión de registro de un nombre de dominio a otro titular que infrinja lo establecido en el presente apartado.

b. Cambio de registradores. Usted no podrá transmitir su registro de nombre de dominio a otro registrador durante un procedimiento administrativo

pendiente iniciado de conformidad con el párrafo 4) durante un período de quince (15) días hábiles (por días hábiles se entenderán los días vigentes en el lugar del domicilio social principal del registrador) la conclusión de dicho procedimiento. Usted podrá ceder la administración de su registro de nombre de dominio a otro registrador durante una acción judicial o arbitraje pendientes, si el nombre de dominio que usted haya registrado ante el registrador sigue estando sujeto a los procedimientos iniciados contra usted de conformidad con las cláusulas de la presente Política. En caso de que usted transmita un registro de nombre de dominio durante el período de resolución de una acción judicial o arbitraje, dicha controversia seguirá estando sujeta a la política sobre controversias en materia de nombres de dominio establecida por el registrador desde el que se haya transmitido el registro del nombre de dominio.

9. Modificaciones de la Política. El registrador se reserva el derecho a modificar en cualquier momento la presente Política con permiso de la ICANN. El registrador publicará la Política revisada en <URL> al menos treinta (30) días naturales antes de su entrada en vigor. Salvo que ya se haya recurrido a la presente Política mediante el sometimiento de una demanda a un proveedor, en cuyo caso a usted se le aplicará la versión de la Política que estaba en vigor en el momento en que se recurrió a ella hasta que finalice la controversia, los cambios efectuados le vincularán con carácter obligatorio en cualquier controversia en materia de registros de nombres de dominio, independientemente de que la controversia haya surgido con anterioridad a la fecha de entrada en vigor del cambio, en dicha fecha o con posterioridad a la misma. En caso de que usted se oponga a un cambio en la presente Política, su único recurso jurídico consistirá en cancelar su registro de nombre de dominio, siempre y cuando no tenga derecho al reembolso de las tasas pagadas al registrador. Asimismo, se le aplicará la Política revisada hasta que cancele su registro de nombre de dominio.

2. Los árbitros

http://www.wipo.int/amc/en/domains/panel/panelists.html#55
puede ahí accederse al listado de panelistas y consultar su perfil.

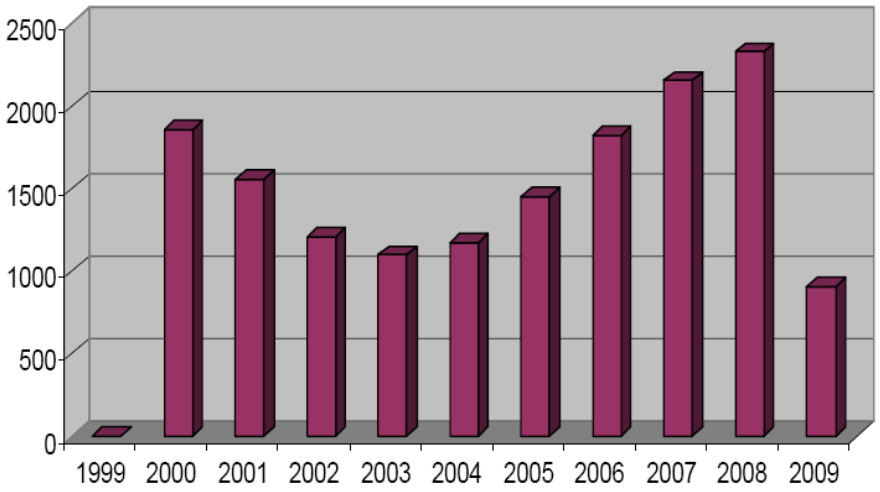
3. Datos sobre los conflictos resueltos por la OMPI 2008

Sacado del interesante artículo OMPI en
http://www.wipo.int/pressroom/en/articles/2008/article_0015.html

¿Alrededor de cuántos casos ha resuelto la OMPI desde 2000? ¿Cuántos casos al año resuelve?
Desde qué país se denuncia más? Y desde España

Qué país se denuncia más? Y España?
Por actividades, qué tres ambitos son los más conflictivos
¿De cada 100 demandas, en cuántas se ordena la transferencia del dominio al demandante?

Número total de casos por año



Year	Number of Cases
1999	1
2000	1857
2001	1557
2002	1207
2003	1100
2004	1176
2005	1456
2006	1824
2007	2156
2008	2329

- **2,329 cases filed in 2008 represent an 8% increase over 2007.**

5

Por país donde está el denunciante

País	Número de Casos	Porcentaje de los asuntos
Estados Unidos de América	5741	44,97%
Francia	1308	10,25%
Reino Unido de Gran Bretaña e Irlanda del Norte	969	7,59%
Alemania	718	5,62%
Suiza	641	5,02%
España	**587**	**4,60%**
Italia	399	3,13%
Canadá	248	1,94%
Australia	224	1,75%
Países Bajos	216	1,69%
Suecia	174	1,36%
Japón	153	1,20%
India	127	0,99%
Dinamarca	104	0,81%
Brasil	102	0,80%

Por país donde está el demandado

País	Número de Casos	Porcentaje de los asuntos
Estados Unidos de América	5125	40,15%
Reino Unido de Gran Bretaña e Irlanda del Norte	1089	8,53%
China	640	5,01%
Canadá	616	4,83%
España	582	4,56%
República de Corea	553	4,33%
Francia	382	2,99%

Australia	300	2,35%
Italia	199	1,56%
Suiza	179	1,40%
Federación de Rusia	175	1,37%
Alemania	171	1,34%
Países Bajos	160	1,25%
India	155	1,21%
Bahamas	147	1,15%

Cuadro 3

GTLDs	Número de nombres de dominio	Porcentaje
. com	2424	73,59%
. NET	287	8,71%
. info	245	7,44%
. org	227	6,89%
. mobi	62	1,88%
. biz	38	1,15%
. nombre	7	0,21%
. cat	4	0,12%

Cuadro 4

Industria y Comercio
(adoptada por el porcentaje de los casos)

Categoy	Porcentaje de casos
Biotecnología y Farmacéutica	10,04%
Banca y finanzas	9,53%
Internet y TI	9,34%
Al por menor	7,76%
Divertirse	7,06%
Alimentación, bebidas y restaurantes	7,03%
Hoteles y Viajes	6,24%
Medios de Comunicación y Publicaciones	6,24%
Moda	6,07%
Telecom	5,29%
Automóviles	4,68%
Electrónica	4,17%
Industria pesada y la maquinaria	3,72%
Otro	3,45%
Transporte	3,10%
Deportes	2,70%
Artículos de Lujo	1,90%
Seguros	1,68%

(traducción automatizada), datos de interés.

En conjunto el número de ccTLD en disputa los nombres de dominio ha sido creciente en los últimos años, habiendo pasado de menos del 1% en el año 2000 a más de 7% en 2007 (Tabla 4). Durante el año pasado el número de registros de ccTLD que han designado a la OMPI que proporcione el nombre de dominio servicios de solución de controversias ha aumentado de 47 a 51 con la adición de Marruecos (. MA), Nauru (. Nr), Perú (. eh), y Santa Lucía (. lc).

Resultados de las controversias

OMPI partes se han asentado de una cuarta parte de todos los casos, sin un panel de decisión. Del resto, el 85% de las decisiones de los paneles han ordenado la transferencia de los nombres de dominio en cuestión para el autor de la queja y el 15% de las quejas se les negó, dejando los nombres en la posesión de la titular del registro. En 2007, los casos se decidieron por 278 expertos de la OMPI nombró procedentes de 42 países.

4. Caso David Bisbal

http://arbiter.wipo.int/domains/

Centro de Arbitraje y Mediación de la OMPI

DECISIÓN DE PANEL ADMINISTRATIVO

David Bisbal Ferré vs. Carlos A. Hurtado Parra

Caso No. D2002-1135

1. Las partes

El Demandante es Don David Bisbal Ferré.

El representante autorizado en este proceso es Doña Olga Arjona Mendoza, con domicilio en Calle Juli Garreta, 1, 17002-Girona, España.

Demandado es Don Carlos A. Hurtado Parra, con domicilio en Calle Calderón de la Barca, 2, 02002-Albacete, España.

El Demandado no se ha personado en el presente procedimiento.

2. Los Nombres de Dominio y el Registro

Los nombres de dominio objeto de la presente demanda, son < davidbisbal.com> , < davidbisbal.net> , < davidbisbal.info> y < davidbisbal.biz> .

La entidad registradora de los citados nombres de dominio es Tucows, Inc., con domicilio en 96 Mowat Avenue, M6K 3M1 Toronto-Canada.

3. Iter procedimental

El Centro de Arbitraje y Mediación de la OMPI (en adelante, el "Centro") recibió el 12 de diciembre de 2002, por correo ordinario, y el 13 de diciembre, por correo electrónico, una demanda (en adelante, la "Demanda"), de acuerdo con la "Política Uniforme de Solución de Controversias en materia de Nombres de Dominio" (en adelante, la "Política Uniforme"), aprobada por la Corporación de Asignación de Nombres y Números de Internet el día 24 de octubre de 1999.

El Centro verificó el cumplimiento en la Demanda de los requisitos formales de la Política Uniforme, el Reglamento de la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (en adelante, el "Reglamento") y el Reglamento Adicional de la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (en adelante, el "Reglamento Adicional").

Tras la verificación registral correspondiente, recibida de la Entidad Registradora el día 13 de diciembre de 2001, la Demanda fue notificada con fecha 17 de diciembre de 2002, al Demandado, dándose por iniciado el procedimiento.

El Demandado no ha contestado a la Demanda.

4. Antecedentes de hecho

El Demandante ha acreditado documentalmente ser el socio único de una sociedad denominada DAVID BISBAL, S.L., consistiendo su objeto social en la gestión de la actividad artística que desarrolla.

El representante artístico del Demandante, la sociedad ACADEMIA DE ARTISTAS, S.L., ha solicitado, en fecha 9 de abril de 2002, la Marca Comunitaria "DAVID BISBAL", para las clases 16, 25 y 41 del Nomenclator Internacional, al efecto de distinguir, entre otros productos y servicios: carteles, cromos, fotografías, etiquetas discográficas, camisetas y prendas de punto, así como servicios de artistas de espectáculos.

A juicio del Panel, en el presente procedimiento merecen ser también tenidas en cuenta las siguientes circunstancias fácticas:

- Los dominios controvertidos < davidbisbal.com> y < davidbisbal.net> fueron registrados el 23 de octubre de 2001, y expiran inicialmente el 23 de octubre de 2004.

- Los dominios controvertidos < davidbisbal.info> y < davidbisbal.biz> fueron registrados el 27 de diciembre de 2001, y expiran inicialmente el 27 de diciembre de 2004.

- En el momento de emisión de la presente decisión, este Panel ha comprobado que, al acceder a los sitios *web* < davidbisbal.com> , < davidbisbal.net> , < davidbisbal.info> y < davidbisbal.biz> aparece una pantalla con la siguiente leyenda: "LO SIENTO ESTA PAGINA HA SIDO CERRADA CAUTELARMENTE". El usuario es redireccionado, en ese momento, al sitio *web* "kantamania.com/triunfo2.htm" a través de una "*pop up*".

- Que el Demandado remitió al Centro un escrito transcurrido el plazo para contestar la Demanda. En este sentido, este Panel quiere poner de relieve que la notificación de la Demanda al Demandado se hizo de acuerdo con los medios previstos en el Reglamento. Así, dice el Párrafo 2 a) i) del Reglamento que "*cuando se transmita*

una demanda al demandado, será responsabilidad del proveedor emplear los medios razonablemente disponibles que se estimen necesarios para lograr que se notifique realmente al demandado. Satisfará esta responsabilidad la notificación efectiva, o el empleo de las siguientes medidas para lograrla", señalando entre ellas, el envío de la demanda en forma electrónica por correo electrónico a las direcciones de correo electrónico para los contactos técnico, administrativo y de facturación. Conforme a lo anterior, el Demandado fue correctamente emplazado y, por consiguiente, su falta de contestación únicamente puede ser imputada a él sin que pueda tener efecto alguno sobre el normal desarrollo de este procedimiento. Asimismo, el escrito presentado por el Demandado no altera ninguno de los términos de la fundamentación realizada por el Panel en la presente decisión.

5. Pretensiones de las partes

5.1. Demandante

El Demandante afirma en su Demanda:

- Que los nombres de dominio controvertidos son idénticos a su nombre artístico, "David Bisbal", nombre que utiliza desde que inició su carrera artística en el mundo de la canción en 1998. Todo ello provocando confusión entre los nombres de dominio controvertidos y el referido nombre artístico.

- Que ha conseguido fama nacional a través del concurso televisivo OPERACIÓN TRIUNFO, cuya primera emisión se produjo el 22 de octubre de 2001, precisamente un día antes de producirse el registro de los nombres de dominio < davidbisbal.com> y < davidbisbal.net> , registrándose un elevado índice de audiencia en la televisión española.

- Que ha intervenido junto con el resto de los participantes del concurso OPERACIÓN TRIUNFO en la grabación de 20 CD's, además de haber grabado un CD en solitario, de gran éxito.

- Que el Demandado carece de derechos e intereses legítimos sobre los nombres de dominio controvertidos, en tanto que no posee ningún derecho de propiedad industrial sobre la denominación "David Bisbal", ni es normalmente conocido bajo la misma.

- Que en los sitios *web* amparados bajo los nombres de dominio controvertidos se explota comercialmente la imagen del Demandante para la venta de obras musicales, así como para lucrarse a través de otros medios como la facturación por llamadas a un número 906, por mensajes SMS Premium, por publicidad en forma de *banners* y venta de productos o servicios relacionados con el Demandante.

- Que los sitios *web* amparados bajo los nombres de dominio controvertidos se presentan como "David Bisbal-Web Oficial" a pesar de que el Demandado no ha sido autorizado por el Demandante ni mantiene ninguna relación ni personal ni profesional con el Demandante que le permitan la explotación de su nombre artístico "David Bisbal" a tal efecto.

- Que los nombres de dominio controvertidos fueron registrados y son utilizados de mala fe, a fin de aprovecharse de la notoriedad del Demandante, atrayendo al mayor número de visitantes posibles con evidente ánimo de lucro, e impidiendo que el

Demandante pueda actuar en el tráfico comercial en Internet a través de su propio nombre artístico.

Como consecuencia de todo ello, el Demandante solicita la transferencia de los dominios controvertidos a su favor.

5.2. Demandado

El Demandado no ha contestado a la Demanda.

6. Debate y conclusiones

6.1 Reglas aplicables

El apartado 15 a) del Reglamento encomienda al Panel la decisión de la Demanda sobre la base de:

- las manifestaciones y los documentos presentados por las partes;

- lo dispuesto en la Política Uniforme y en el propio Reglamento; y

- de acuerdo con cualesquiera reglas y principios de Derecho que el Panel considere aplicables.

Teniendo en cuenta la común residencia en España de Demandante y Demandado son de especial relevancia, junto con las reglas de la Política Uniforme, las leyes y principios del Derecho nacional español. En este sentido, en particular, entiende el Panel atendible lo dispuesto tanto en la legislación sobre signos distintivos como en el ordenamiento contra la competencia desleal.

6.2 Examen de los presupuestos para la estimación de la Demanda contenidos en el apartado 4 a) de la Política Uniforme

Éstos son:

- que el nombre de dominio registrado por el demandado sea idéntico, u ofrezca semejanza que produzca confusión, con una marca de productos o servicios sobre la que el demandante tenga derechos;

- que el demandado carezca de derecho e interés legítimo en relación con el nombre de dominio; y

- que el nombre de dominio haya sido registrado y usado de mala fe.

6.3. Identidad o semejanza entre marca y dominio

Existe plena identidad entre los dominios controvertidos y la denominación "David Bisbal", descontando obviamente en la confrontación el sufijo "com" (entre otros, caso OMPI D2000-0834, D2001-0017).

Así pues, el Panel considera probada la concurrencia del requisito exigido por el artículo 4 a) i) de la Política Uniforme.

6.4. Inexistencia de un interés legítimo del Demandado en relación con los nombres de dominio controvertidos y consecuente constatación de mala fe en el registro de los mismos

Ha sido la sociedad ACADEMIA DE ARTISTAS, S.L., y no el Demandante, quien ha procedido a la solicitud de una Marca Comunitaria para la denominación "David Bisbal". Esta circunstancia, sin embargo, no debe menospreciarse pues, como se

verá, posee relevancia en la evaluación de la conducta de cuidado desplegada por el Demandante en cuanto a la explotación comercial de su nombre artístico.

Y en todo caso, entiende el Panel que la apenas citada circunstancia no priva al Demandante de legitimidad para interponer su reclamación. En este sentido, es conocida la doctrina de este Centro por cuya virtud, en atención a determinados hechos, se atribuye excepcionalmente protección a los nombres de personas físicas claramente asociables por el público con el ejercicio de una actividad profesional, con el acertado propósito de impedir una explotación abusiva o de mala fe por parte de terceros que persiguen enriquecerse injustamente (entre otros, casos, OMPI D2000-0210, *Julia Roberts vs. Russell Boyd*, OMPI D2000-0794, *Helen Folsade Adu conocida como SADE vs. Quantum Computer Services, Inc.*, OMPI D2000-0847, *Madonna Ciccone, p/k/a Madonna vs. Dan Parisini*, OMPI D2000-0867, *Isabelle Adjani vs. Second Orbit Communications, Incs.*). La referida doctrina se ha perfilado ulteriormente en el sentido de que la notoriedad asociada a un nombre bajo el que se realiza una actividad profesional o comercial genera una suerte de derecho consuetudinario sobre el mismo (entre muchas otras: OMPI D2000-1649, *Rosa Montero Gallo vs. Galileo Asesores, S.L.*, OMPI D2000-1650, *José Luis Sanpedro vs. Galileo Asesores, S.L.*, u OMPI D2001-0121, *Julian Barnes vs. Old Barn Studios Limited,* OMPI D2001-0710, *Xavier Hernández Creus vs. Isidro Sentis Sales*). La tutela que la Política confiere a los signos distintivos registrados se extiende, así, a las llamadas *marcas de hecho*, constituidas por denominaciones coincidentes con nombres de personas físicas a las que el público vincula inmediatamente con el ejercicio de una actividad profesional o bien económica, por ser tal asociación notoria; y todo ello sin perjuicio de que dichos nombres no estén protegidos por una marca registrada.

El Demandante, conocedor de tal doctrina, ha proporcionado al Panel abundante documentación acreditativa de la notoriedad alcanzada por su persona, en tanto que artista profesional, en el territorio español. Si bien el Panel acepta, en línea de principio, el argumento del Demandante, considera oportuno realizar una precisión de la que derivan a su vez implicaciones importantes en cuanto a la calificación jurídica de los hechos controvertidos: de la propia documentación aportada por el Demandante se desprende que la notoriedad alegada se ha ido desarrollando, al menos a nivel nacional, en un plazo relativamente corto de tiempo, a partir de la emisión del programa televisivo "OPERACIÓN TRIUNFO". Ello dificulta, en principio, el análisis de si concurría en el Demandado mala fe en el momento del registro de los dominios controvertidos, o al menos de los prioritarios en el tiempo (< davidbisbal.com> y < davidbisbal.net>). Sin embargo, una vez sopesadas todas las circunstancias que rodean al caso, este Panel entiende que el Demandado ha actuado de mala fe tanto en el momento del registro como en el posterior uso de todos y cada uno de los dominios en conflicto. Sobre este segundo aspecto volveremos más adelante.

En esta fase del procedimiento, toca analizar si el Demandado se hallaba o no investido de un interés legítimo en el momento de solicitar el registro de los dominios controvertidos. En principio, el Demandado no ha aportado prueba alguna (pues no ha contestado a la Demanda) de poseer ningún derecho en respaldo de los registros efectuados: ni posee una marca, ni coinciden los dominios con su propio nombre, ni tampoco cuenta en su haber con una autorización del Demandante que le habilite al efecto. Por el contrario, y a partir de las alegaciones del Demandante, queda

demostrado que el Demandado no procedió a recabar en ningún momento la autorización de aquél para la utilización de su nombre artístico.

Entiende este Panel que el hecho de que un personaje de cierta fama no haya procedido a proteger su nombre en el ámbito Internet no concede una patente de corso para que un tercero se lo apropie. O, al menos, no ha de ocurrir cuando, como aquí ocurre, el nombre es distintivo en tanto que el público lo asocia con el Demandante y su prestación artística y, sobre lo anterior, de los actos del afectado puede deducirse su voluntad de controlar la explotación económica asociada a su imagen e identidad. Ciertamente, esta voluntad se aprecia en el caso que nos ocupa, en atención, de un lado, al hecho de que el Demandante sea socio de la sociedad cuyo objeto es, precisamente, gestionar su actividad artística y, de otro lado, al hecho de que alegue en defensa de su posición que su representante, la sociedad ACADEMIA DE ARTISTAS, S.L., ha procedido a realizar (obviamente, con su autorización) una solicitud de marca denominativa coincidente, en su composición, con su nombre y primer apellido. Por lo demás, parece asimismo relevante atender a la rápida reacción del Demandante: bajo este aspecto, se convendrá que no puede merecer igual protección quien se ocupa con presteza de proteger su nombre que quien tolera durante largo tiempo la usurpación del mismo.

Advertido lo anterior, entiende el Panel que el Demandado actuó en todo caso de mala fe, concretándose ésta en una clara voluntad (oportunista) de obstaculizar en el mercado el legítimo aprovechamiento por parte del Sr. David Bisbal de las futuras oportunidades económicas ligadas a la explotación comercial del propio nombre artístico en la red Internet. Bajo este aspecto, y aunque a fecha 23 de octubre de 2001, (recuérdese, un día después de emitirse el primer episodio del programa-concurso "OPERACIÓN TRIUNFO"), el Sr. David Bisbal no gozara quizás de una popularidad consolidada a nivel nacional, no puede desconocerse la repercusión social, al menos en el territorio español, que este tipo de programas posee y, con ello, el evidente potencial de notoriedad que gravita sobre quienes participan en los mismos. Se da, además, la circunstancia de que la futura emisión del programa televisivo en cuestión se había apoyado con una campaña multimedia de fuerte impacto, lo que había generado cierta expectación entre el público y, desde luego, había supuesto la difusión de la identidad y perfil de los concursantes. Desde esta perspectiva, el registro de los nombres de dominio < davidbisbal.com> y < davidbisbal.net> no puede reputarse casual, sino orientado a una ocupación ilegítima de los mismos.

Es evidente, en este caso, el doloso propósito especulativo del Demandado, el cual procedió a registrar el dominio a sabiendas de que, en un plazo inmediato, podía asociarse al mismo una rentabilidad económica proveniente de los esfuerzos de un tercero. En este sentido, debe recordarse la doctrina de este Centro que declara irrelevante, a efectos de valorar el carácter ilegítimo del registro, constatar si el Demandado tenía la intención de aprovecharse de una marca ya registrada, o bien de un derecho marcario de cuyo nacimiento conocía o estaba en condiciones de conocer (así, caso OMPI D2002-0669, *Execuject Holdings Ltd. vs. Air Alpha America, Inc.*). Analizados ahora estos hechos a la luz de la cláusula general de la Ley 3/1991, de 10 de enero, de Competencia Desleal, no ofrecería duda su calificación como un acto de obstaculización u obstrucción.

Ulteriormente, entiende el Panel que la reincidencia del Demandado, poco tiempo después, con ocasión del registro de los otros dos nombres de dominio < davidbisbal.info> y < davidbisbal.biz> , confirma aquella calificación en tanto que evidencia el oportunista propósito de ocupar en la red el máximo espacio en el que podría utilizarse comercialmente la identidad del Sr. David Bisbal. En efecto, si a fecha 23 de octubre de 2001, era obvio el potencial mediático del Sr. David Bisbal, el 27 de diciembre de 2001, éste ya no podía ignorarse en absoluto.

Así las cosas, entiende este Panel que procede una consideración unitaria de todos los dominios controvertidos: y ello, no por constituir todos ellos objeto de un mismo procedimiento, sino porque resulta razonable presumir que su registro responde a un mismo patrón de conducta, el cual viene de algún modo confirmado por la actitud pasiva del Demandado en este procedimiento. En efecto, el hecho de que el Demandado no haya contestado la Demanda autoriza a extraer alguna conclusión, siquiera indiciaria, sobre este extremo (en línea con lo mantenido por el Panel en el caso OMPI D2001-0003).

En definitiva, este Panel considera que, aún a pesar de que el Demandante no posea un derecho de marca sobre su nombre y de que quizá, a fecha 23 de octubre de 2001, no gozara todavía de un renombre indiscutible en todo el territorio nacional (aunque sí, según parece, a nivel regional), resulta incuestionable que una parte muy notable del público español conocía de su existencia y de su potencial celebridad en un futuro inmediato, desde luego constatable ya en fecha de la segunda tanda de registros. Y entre tales espectadores se hallaba, en buena lógica, el Demandado, quien está domiciliado en territorio español al igual que el Demandante. Así las cosas, entiende el Panel que el Demandado carecía de interés legítimo en relación con todos y cada uno de los nombres de dominio controvertidos y que, sobre lo anterior, los registró con evidente propósito oportunista y, por lo tanto, de mala fe.

De todas las consideraciones que anteceden se sigue que el Panel considera probada la concurrencia del requisito exigido por el artículo 4 en sus apartados a) ii) y b ii) de la Política Uniforme.

6.5. Existencia de mala fe en el uso de los dominios controvertidos

Es conocida la doctrina mantenida por el Panel en anteriores ocasiones (entre otras, con motivo de las decisiones OMPI D2000-0239, D2000-1354, D2001-0397, D2001-0773 y D2001-0780), por cuya virtud cabe presumir que, en buena lógica, quien registró el dominio de mala fe y sin interés legítimo, lo usará probablemente también de mala fe. Este caso confirma esta presunción, a contrario, por cuanto el uso de mala fe de los dominios viene a consolidar que su registro no pudo sino efectuarse de mala fe, una vez acreditado que el registrante carecía de un interés legítimo en aval de su posición.

El referido uso de mala fe se ha manifestado, por lo demás, en dos tiempos. En un primer momento, conforme a la prueba documental aportada por el Demandante, en los sitios *web* amparados bajo los nombres de dominio controvertidos, el Demandado ha explotado la imagen y el nombre artístico del Demandante, en su propio beneficio, para la venta de obras musicales, así como para lucrarse a través de otros medios como la facturación por llamadas a un número 906, por mensajes SMS Premium, por publicidad en forma de *banners* y venta de productos o servicios relacionados con el Demandante,

sin que el Demandado haya sido en momento alguno autorizado por el Demandante al efecto.

En la actualidad, el Panel ha podido constatar que, al intentar acceder a los sitios *web* < davidbisbal.com> , < davidbisbal.net> , < davidbisbal.info> y < davidbisbal.biz> , aparece una pantalla con la siguiente leyenda: "LO SIENTO ESTA PAGINA HA SIDO CERRADA CAUTELARMENTE". Sin embargo, el usuario es entonces redireccionado al sitio *web* "kantamania.com/triunfo2.htm" a través de una "*pop up*" en el que oferta la venta de la colección completa de las canciones del concurso televisivo OPERACIÓN TRIUNFO, entre las que se incluyen las del Demandante.

La conducta del Demandado, es indudable, se ha dirigido y dirige a promover una asociación deliberada y abusiva en la presentación de su oferta en el mercado con los servicios o prestaciones propios del Demandante, propósito que es tanto más evidente, existiendo, como existe, una conexión inmediata entre la actividad del Demandante y la propia del Demandado.

A la luz de la normativa española contra la competencia desleal, los anteriores hechos son subsumibles en los supuestos tipificados en los artículos 6 y 12 de la referida Ley que prohíben, respectivamente, los actos de confusión y la explotación de la reputación ajena.

Así, mientras que el artículo 6 considera desleal "*todo comportamiento que resulte idóneo para crear confusión de la actividad, las prestaciones o el establecimiento ajenos. El riesgo de asociación por parte de los consumidores respecto de la procedencia de la prestación es suficiente para fundamentar la deslealtad de una práctica*", el artículo 12 reputa desleal "*el aprovechamiento indebido, en beneficio propio o ajeno, de las ventajas de la reputación industrial, comercial o profesional adquirida por otro en el mercado*".

Por consiguiente, el Panel concluye que también concurre en el presente supuesto el requisito exigido por el artículo 4 a) iii) de la Política Uniforme.

7. Decisión

El Panel, considerando probado que los nombres de dominio < davidbisbal.com> , < davidbisbal.net> , < davidbisbal.info> y < davidbisbal.biz> son todos y cada uno idénticos al nombre artístico del Demandante, que el Demandado carece de derechos o intereses legítimos respecto de los nombres de dominio objeto de la presente controversia y que éstos fueron registrados y se usan de mala fe, resuelve que procede estimar la Demanda y requiere que el registro de los nombres de dominio < davidbisbal.com> , < davidbisbal.net> , < davidbisbal.info> y < davidbisbal.biz> se transfieran al Demandante.

Paz Soler Masota

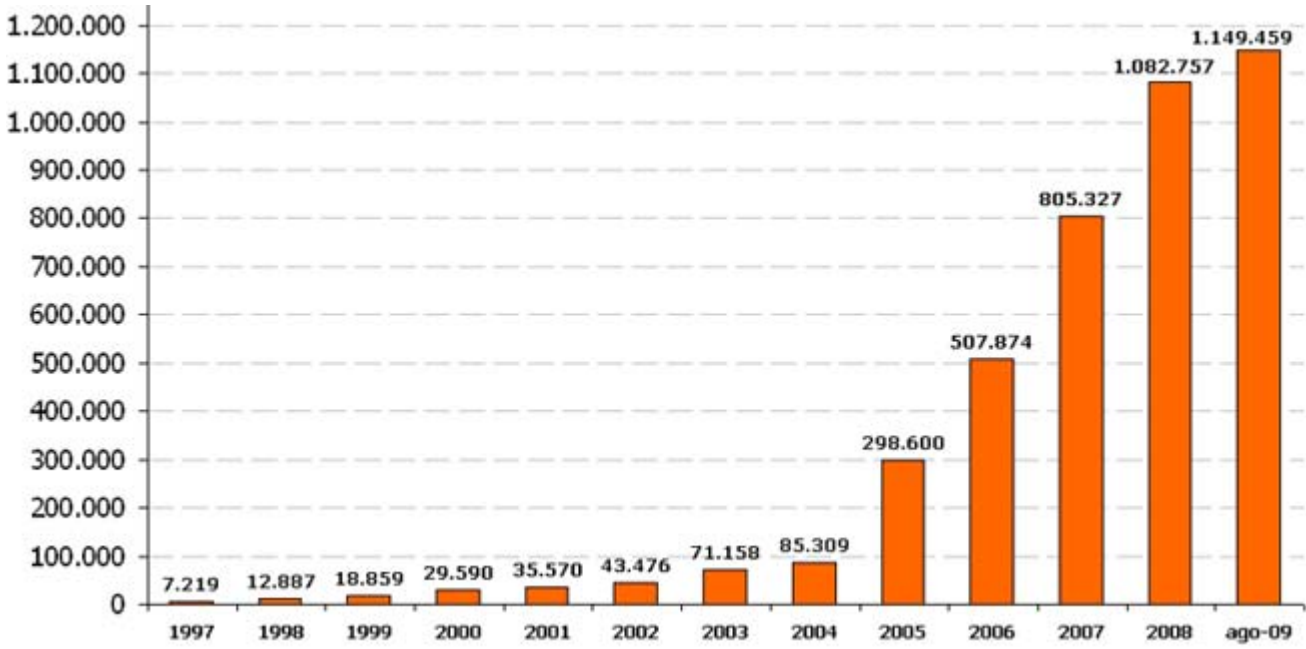
Panelista Único

Fecha: 24 de enero de 2003

2. Dominio .es

ver www.nic.es

1. Estadísticas: dominios registrados en los últimos años



2. Qué se puede registrar y cómo

Sobre el precio, tú mismo puedes comparar el precio "oficial" (www.nic.es) y el de libre mercado, por ejemplo www.piensasolutions.es)

Puede solicitar cualquiera de los siguientes dominios con total libertad:

- **Dominios que se asignan de forma automática:**
  - ".es", para identificar su nombre, su empresa, su organismo en Internet. Ejemplos:
    - loquequiera.es
    - minombre.es
    - miempresa.es
    - miorganismo.es
  - ".com.es" para cualquier tipo de actividad a un precio muy reducido, por ejemplo concierto.com.es
  - ".nom.es", para tu nombre, por ejemplo martaperez.nom.es
  - ".org.es" para tu organización ejemplo caritas.org.es
- **Dominios que requieren verificación previa :**

- Los dominios ".gob.es" y ".edu.es" facilitarán a Organismos Públicos y Entidades e Instituciones relacionadas con la Enseñanza o la Investigación en España su identificación en Internet. Estos dominios requieren una verificación previa, requiriendo un plazo máximo de 24 horas para su registro.
    - ".edu.es" si eres una organización educativa, oficialmente reconocida, por ejemplo colegioxxx.edu.es
    - ".gob.es" Reservado a instituciones gubernamentales, por ejemplo ministerio.gob.es

Su dominio ".es" será asignado de acuerdo al orden de llegada, por ello el primer solicitante será el primero en obtenerlo, además debe tener en cuenta que:

- Que no esté asignado con anterioridad.
- Que cumpla con las normas de sintaxis.
- Que no esté incluido en la lista de términos prohibidos.
- Que no esté incluido en la lista de términos reservados.

3. Normativa reciente: Plan de dominios

El 1 de Junio de 2005 entró en vigor la Orden Ministerial ITC/1542/2005, de 19 de mayo, por la que se aprueba el Plan Nacional de Nombres de dominio de Internet bajo el Código correspondiente a España (".es").

Este Plan tiene por objeto flexibilizar por completo la normativa vigente referente a la asignación de nombres de dominio bajo ".es".

Algunos de los aspectos más relevantes son:

- Un dominio se asigna de forma automática si se encuentra libre (salvo .gob.es y .edu.es).
- Cualquier persona física o jurídica con intereses o vínculos con España tiene derecho a obtener el dominio.
- Se han eliminado distintas restricciones que se contemplaban anteriormente.

El Plan Nacional de nombres de dominio prevé, en su apartado Séptimo, la aprobación por la Entidad Pública Empresarial Red.es de una lista de términos prohibidos y tres listas de términos reservados.

Dichas listas fueron aprobadas por Instrucción del Presidente de la Entidad Pública Empresarial Red.es de fecha 12 de Septiembre de 2005, las cuales en virtud de lo dispuesto en el apartado cuarto de la misma, han sido completadas y actualizadas por Instrucción del Director General de Red.es de 28 de junio de 2006.

Las listas aprobadas son las siguientes:

- La lista de términos prohibidos incluye una relación reducida y actualizada de términos de Internet cuyo uso como nombre de dominio, al poder generar confusión, está prohibido.

- Las listas de términos reservados, relativas a nombres de dominio de segundo nivel que no podrán ser objeto de asignación libre, son tres:
  - La primera, otorga el carácter de reservados a una relación de nombres de dominio relativos a denominaciones de órganos constitucionales u otras instituciones del Estado, así como términos relativos a la Casa Real que no hayan sido previamente asignados o que queden vacantes.
  - La segunda otorga el carácter de reservados a nombres de dominio relativos a denominaciones de organizaciones internacionales y supranacionales oficialmente acreditadas, que no hayan sido previamente registrados o que queden vacantes.
  - La tercera otorga el carácter de reservados a una relación actualizada de nombres de dominio consistentes en topónimos que coincidan con la denominación oficial de Administraciones públicas territoriales y que no hayan sido previamente asignados, o que queden vacantes. Asimismo se incluye una lista correspondiente a topónimos o gentilicios que figuran en la lista ISO 3166-1 en sus versiones oficiales y en su traducción al castellano.

4. Extractos de la normativa actual (Orden de mayo 2005) que ha variado todo

ORDEN ITC/1542/2005, de 19 de mayo, que aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («.es»).

PLAN NACIONAL DE NOMBRES DE DOMINIO DE INTERNET BAJO EL CÓDIGO DE PAÍS CORRESPONDIENTE A ESPAÑA («.ES»)

Asignación de nombres de dominio de segundo nivel

Quinto. Criterio general de asignación de nombres de dominio de segundo nivel.

–Los nombres de dominio de segundo nivel bajo el «.es» se asignarán atendiendo a un criterio de prioridad temporal en la solicitud. No podrán ser objeto de solicitud nombres de dominio que ya hayan sido previamente asignados. Los nombres de dominio de segundo nivel bajo el «.es» se asignarán sin comprobación previa, salvo en lo relativo a las normas de sintaxis recogidas en el punto 1 del apartado undécimo, la lista de términos prohibidos prevista en el punto 2 del apartado undécimo y las limitaciones específicas y las listas de nombres de dominio de segundo nivel prohibidos o reservados recogidas en el apartado séptimo.

Sexto. Legitimación para la asignación de nombres de dominio de segundo nivel.–Podrán solicitar la asignación de un nombre de dominio de segundo nivel las personas físicas o jurídicas y las entidades sin personalidad que tengan intereses o mantengan vínculos con España.

Duodécimo. Transmisión de los nombres de dominio.

1. El derecho a la utilización de un nombre de dominio podrá ser transmitido voluntariamente, siempre y cuando el adquirente cumpla con lo previsto en este Plan y en su normativa de desarrollo. Toda transmisión voluntaria deberá contar con la aprobación del antiguo titular del nombre de dominio, que deberá ser comunicada a la autoridad de asignación con carácter previo a la correspondiente modificación de los datos de registro del nombre de dominio. Dicha aceptación deberá ser formalizada por el antiguo titular de acuerdo con los procedimientos que establezca la autoridad de asignación.

2. En los casos de sucesión universal «inter vivos» o «mortis causa» y en los de cesión de la marca o nombre comercial al que estuviera asociado el nombre de dominio, el sucesor o cesionario podrá seguir utilizando dicho nombre, siempre que cumpla las normas de asignación de nombres de dominio recogidas en este Plan y solicite de la autoridad de asignación la modificación de los datos de registro del nombre de dominio.

Decimotercero. Derechos y obligaciones derivados de la asignación y mantenimiento de los nombres de dominio.

1. Los solicitantes de un nombre de dominio deberán facilitar sus datos identificativos siendo responsables de su veracidad y exactitud.

2. La asignación de un nombre de dominio confiere el derecho a su utilización a efectos de direccionamiento en el sistema de nombres de dominio de Internet en los términos señalados en este Plan y a la continuidad y calidad del servicio que presta la autoridad de asignación.

3. Los beneficiarios de un nombre de dominio bajo el «.es» deberán 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».

4. Los usuarios de un nombre de dominio deberán informar inmediatamente a la autoridad de asignación de todas las modificaciones que se produzcan en los datos asociados al registro del nombre de dominio.

5. El derecho a la utilización del nombre de dominio estará condicionado al respeto a las obligaciones contenidas en este apartado decimotercero, a las normas recogidas en el apartado undécimo y al mantenimiento de las demás condiciones aplicables. El incumplimiento de lo anterior determinará su cancelación por la autoridad de asignación, a través del procedimiento y dentro de los plazos que establezca la autoridad de asignación en los términos previstos en la disposición adicional decimoctava de la Ley 14/2000, de 29 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. En este procedimiento deberá ser oído siempre el beneficiario del nombre de dominio.

La autoridad de asignación podrá comprobar en cualquier momento, de oficio o a instancia de parte, si se mantienen las condiciones para la asignación de un nombre de dominio.

En los procedimientos iniciados a instancia de parte, la única pretensión que podrá ejercitarse será la de la cancelación del nombre de dominio por incumplimiento

de alguna de las condiciones generales a que está sometida su asignación referidas en este Plan, sin perjuicio del derecho de las partes a acudir a la jurisdicción competente.

La persona o entidad que haya instado la iniciación del procedimiento tendrá preferencia para la obtención del nombre de dominio, si presenta su solicitud en el plazo que se establezca en las normas de procedimiento.

6. Los cambios de prestador de servicios o la conexión simultánea a varios prestadores no alteran la asignación y mantenimiento de un nombre de dominio.

7. Los titulares de nombres de dominio de segundo o tercer nivel se someterán al sistema de resolución extrajudicial de conflictos previsto en la disposición adicional única, sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

Decimocuarto. Responsabilidad por la utilización de nombres de dominio.

1. La responsabilidad del uso de un nombre de dominio y el respeto a los derechos de propiedad intelectual e industrial corresponde a la persona u organización a la que se haya asignado dicho nombre de dominio.

2. Los agentes registradores acreditados no son responsables de la utilización de los nombres de dominio asignados a las organizaciones o personas a las que presten los servicios previstos en esta Orden.

Disposición adicional única. Sistema de resolución extrajudicial de conflictos.

Como complemento a este Plan y en los términos que permitan las disposiciones aplicables, la autoridad de asignación establecerá un sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio en relación con, entre otros, los derechos de propiedad industrial protegidos en España, tales como los nombres comerciales, marcas protegidas, denominaciones de origen, nombres de empresas; o con las denominaciones oficiales o generalmente reconocibles de Administraciones Públicas y organismos públicos españoles. Este sistema de resolución extrajudicial de conflictos se basará en los siguientes principios:

a) Deberá proporcionar una protección eficaz frente al registro de nombres de carácter especulativo o abusivo, en especial cuando el nombre de dominio sea idéntico o similar hasta el punto de crear confusión con otro término sobre el que exista algún derecho previo de los citados en el párrafo anterior.

b) Se entenderá que existe un registro especulativo o abusivo cuando el titular del dominio haya registrado el mismo careciendo de derechos o intereses legítimos sobre el nombre de dominio en cuestión y haya sido registrado o se esté utilizando de mala fe.

c) La participación en el sistema de resolución extrajudicial de conflictos será obligatoria para el titular del nombre de dominio.

d) La autoridad de asignación podrá acreditar a proveedores de servicios de solución extrajudicial de conflictos basándose en condiciones proporcionadas, objetivas, transparentes y no discriminatorias que garanticen su cualificación y

experiencia en el campo de la resolución extrajudicial de conflictos. La autoridad de asignación mantendrá en su página de Internet la relación de proveedores acreditados.

e) Los resultados del sistema extrajudicial de resolución de conflictos serán vinculantes para las partes y para la autoridad de asignación, a no ser que se inicien procedimientos judiciales en el plazo de treinta días naturales a partir de su notificación a las partes.

f) La persona o entidad que haya instado la iniciación del procedimiento tendrá preferencia para la obtención del nombre de dominio, si presenta su solicitud en el plazo que se establezca en las normas de procedimiento.

g) El sistema extrajudicial de resolución de conflictos deberá asegurar a las partes afectadas las garantías procesales adecuadas y se aplicará sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar. La autoridad de asignación dará publicidad de modo periódico y actualizado a los nombres de dominio asignados, a fin de facilitar el ejercicio de los derechos tutelados por el sistema de resolución extrajudicial de conflictos.

5. Conflictos y Recuperación del domino.es

Recupere su dominio: Derechos previos

Podrán hacer uso del Sistema de Resolución extrajudicial de conflictos para nombres de dominio bajo el código de país correspondiente a España ".es", toda persona física o entidad con o sin personalidad jurídica que ostente alguno de los siguientes derechos previos:

1. Denominaciones de entidades válidamente registradas en España, denominaciones o indicaciones de origen, nombres comerciales, marcas registradas u otros derechos de propiedad industrial protegidos en España.
2. Nombres civiles o seudónimos notorios, que identifiquen profesionalmente, entre otros, a creadores intelectuales, políticos y figuras del espectáculo o del deporte.
3. Denominaciones oficiales o generalmente reconocibles de Administraciones Públicas y organismos públicos españoles.

---

reglamento disponible en

https://www.nic.es/normativa/instruccion/descargables/resolucion_dominios.pdf

6. Procedimiento

El sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio ".es", desarrollado por la entidad pública empresarial Red.es, se basa en la prácticas generalmente aplicadas en el ámbito internacional, y las recomendaciones emanadas por las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Es necesario poseer derechos previos de un nombre de dominio ".es" ya asignado, para hacer uso de dicho sistema, de acuerdo a lo establecido en el Reglamento del Procedimiento de Resolución extrajudicial de conflictos, aprobado el 7 de noviembre de 2005.

Se deben acreditar los motivos por los que el registro del nombre de dominio ".es" es de carácter especulativo o abusivo, y en particular:

- Los motivos por los que el nombre de dominio ".es" es idéntico o similar hasta el punto de crear confusión con otro término sobre el que el Demandante alega poseer Derechos Previos; y
- Los motivos por los que debe considerarse que el Demandado carece de derechos o intereses legítimos sobre el nombre o nombres de dominio objeto de la demanda; y
- Los motivos por los que debe considerarse que el nombre de dominio ha sido registrado o se esté utilizando de mala fe.

En todo caso, la demanda debe ser instada ante un Proveedor de resolución extrajudicial de conflictos acreditado por la entidad pública empresarial Red.es, de acuerdo al artículo 13 del Reglamento del Procedimiento de Resolución extrajudicial de conflictos.

En el sistema de resolución extrajudicial de conflictos de nombres de dominio ".es", hay varios roles, que es conveniente conocer:

- Entidad pública empresarial Red.es, en este caso sus funciones son básicamente, velar por el cumplimiento de las obligaciones de los Proveedores, y ejecutar las resoluciones establecidas por el experto.
- Proveedor, organización sin ánimo de lucro que administra las demandas, y vela por la tramitación de las mismas de acuerdo a lo establecido en el Reglamento, nombrado al Experto con imparcialidad e independencia.
- Partes: demandante, persona física u organización que insta la demanda ante el proveedor contra el demandado, titular del nombre de dominio ".es" objeto de la controversia.
- Experto: profesional con experiencia acreditada en resolución extrajudicial de conflictos, que resolverá la controversia con el máximo rigor e independencia, teniendo en cuenta el contenido de la demanda y la contestación a la misma.

No podrá ser iniciado el procedimiento de resolución extrajudicial de conflictos cuando se encuentre abierto un procedimiento de cancelación del nombre de dominio ".es". En todo caso la vía judicial está siempre abierta para las Partes, independientemente del estado de la demanda.

La tarifa establecida por los proveedores de resolución extrajudicial de conflictos de nombres de dominio ".es" es de **1.400€**.

Para resolver la demanda el experto tendrá en cuenta las declaraciones y documentos presentados por las partes.

El experto, en un plazo medio de 2 MESES desde la interposición de la demanda, resolverá mediante resolución motivada que debe ser congruente con la pretensión de la demanda y no podrá decidir sobre cuestiones ajenas a la misma.

En base al artículo 13 de la instrucción por la que se regula el DRP el demandante deberá indicar en la demanda la pretensión que se pretende obtener, es decir la transmisión del nombre de dominio al demandante o la cancelación del mismo.

Por tanto el experto puede resolver:

- **Estimar la demanda**
- **En este caso el experto puede acordar:**
    1. **Transmitir el nombre de dominio al demandante.** En este supuesto, transcurrido el plazo máximo de un mes a partir de la notificación de la decisión a las partes y Red.es, el demandante deberá enviar una solicitud de transmisión a transmisionDRP@nic.es. Recibida dicha solicitud se realizara la transmisión del nombre de dominio al demandante.
    2. Solicitud de transmisión en cumplimiento de la resolución dictada en el procedimiento de resolución extrajudicial de conflictos:
        - Para dominio gestionado por usuario final
        - Autorización a Agente Registrador para actuar por cuenta del asignatario
    3. **Cancelar el nombre de dominio, que quedará para libre asignación.** En el caso de que el demandante no haya indicado en la demanda que quiere la transmisión del nombre de dominio objeto de la controversia.

- **No estimar la demanda**. En este supuesto el experto considera que el demandado tiene razón y por tanto el nombre de dominio debe continuar asignado a favor del antiguo titular.

Si en el citado plazo de 30 días, cualquiera de las partes notificará a Red.es un documento acreditando que se ha iniciado un procedimiento judicial ante un juzgado competente, Red.es suspenderá la ejecución de la decisión hasta que reciba comunicación de que ha concluido dicho procedimiento judicial, salvo que el órgano judicial determine lo contrario.

7. Resolución de árbitro en conflicto .es: caso open-bank.es

DECISION DEL EXPERTO

Open Bank Santander Consumer, S.A v. Cibergirona, S.L.

I. Antecedentes de Hecho.

1) Las Partes.

Demandante: Open Bank Santander Consumer, S.A., con domicilio en XXX.

El representante autorizado por la demandante es Dª C.H.L., con el mismo domicilio.

Demandado: Cibergirona, S.L., con domicilio en XXX.

2) El Nombre de Dominio y el Registro.

La demanda tiene como objeto el nombre de dominio **<open-bank.es>.**

El nombre de dominio se ha registrado ante la entidad pública empresarial Red.es.

3) Iter Procedimental.

La demanda se presentó ante la Asociación para la Autorregulación de la Comunicación Comercial ("Autocontrol") el 10 de abril de 2006. De conformidad con lo establecido en las Normas de Procedimiento de Resolución Extrajudicial de Conflictos para Nombres de Dominio bajo el código de país correspondiente a España (".ES") (las "Normas de Procedimiento") y en el Reglamento del Procedimiento de Resolución Extrajudicial de Conflictos de Nombres de Dominio bajo el código de país correspondiente a España (".es") (el "Reglamento"), la Secretaría de "Autocontrol" notificó la demanda a la demandada.

La demandada no ha contestado a la demanda.

El Director General de "Autocontrol" designó a D. Alberto Bercovitz como Experto único, recibiendo la "Declaración de Aceptación y de Imparcialidad", de conformidad con el artículo 17 de las "Normas de Procedimiento". El Experto Único considera que su nombramiento se ajusta a las normas del procedimiento.

1

4) Hechos relevantes.

La demandante es la entidad de crédito Open Bank Santander Consumer, S.A., inscrita en el Registro de bancos y Banqueros del Banco de España (Registro Mercantil de Madrid, hoja nº 78.974, Folio I, Tomo 8.269).

Esta sociedad es titular registral del Nombre Comercial nº 209.293 "OPENBANK", solicitado el 8 de julio de 1996; de las Marcas Españolas nº 1.802.711 "OPEN BANK", nº 2.625.917 "OPENBANK" (mixta); y nº 2.656.262 "OPENBANK" (mixta), solicitada el 9 de junio de 2005; y de las Marcas Comunitarias nº 1.567.338 "OPENBANK" (mixta); nº 308.528 "OPEN BANK" (mixta), solicitada el 1 de julio de 1996; y de la solicitud de registro de Marca Comunitaria nº 4.482.493 "OPENBANK" (mixta).

Aunque la demandante no ha aportado prueba alguna que acredite el conocimiento de la marca en el mercado, al Experto le consta personalmente que la demandante ha venido haciendo un uso continuado de estas marcas en campañas publicitarias de sus productos y servicios, tanto en prensa como en radio y televisión y como

consecuencia de este uso OPENBANK con el que esta entidad de crédito es conocida en el mundo financiero.

La demandada es la sociedad Cibergirona, S.L.

El nombre de dominio <open-bank.es> fue registrado por la sociedad Cibergirona, S.L. el 21 de noviembre de 2005.

Con fecha 5 de diciembre de 2005, la demandada dirigió un correo electrónico a la demandante presentándose como una empresa que ofrece servicios de pre-registro de dominios de denominación ".es" a empresas españolas a fin de evitar registros indeseados y ofreciendo la transferencia del nombre de dominio. La sociedad demandada tiene registrados otros muchos nombres de dominio, algunos de los cuales identifican entidades financieras españolas muy conocidas. Todos estos registros se han realizado mediante el sistema de introducir un guión intermedio en el nombre. En concreto, Cibergirona, S.L. tiene registrados los nombres de dominio: <banca-march.es>, <ban-caja.es>, <banco-esfinge.es>, <banco-etchevarria.es>, <banco-gallego.es>, <banco-herrero.es>, <banco-pastor.es>, <banc-sabadell.es>, <sabadell-atlantico.es>, <caja-circulo.es>, <caixa-girona.es>, caixa-penedes.es>, <caja-canarias.es>, <lloyds-bank.es>, <sol-bank.es>, <uni-caja.es>, <banco-urquijo.es>.

El Experto ha podido comprobar personalmente, que a la fecha de esta Resolución, el nombre de dominio <open-bank.es> remite a una página de contenido general del Agente Registrador Acens.

2

5) Alegaciones de las partes.

A. Demandante.

En su escrito de demanda la demandante afirma:

- La sociedad Open Bank Santander Consumer, S.A es titular registral del Nombre Comercial nº 209.293 "OPENBANK", solicitado el 8 de julio de 1996; de las Marcas Españolas nº 1.802.711 "OPEN BANK", nº 2.625.917 "OPENBANK" (mixta); y nº 2.656.262 "OPENBANK" (mixta), solicitada el 9 de junio de 2005; y de las Marcas Comunitarias nº 1.567.338 "OPENBANK" (mixta); nº 308.528 "OPEN BANK" (mixta), solicitada el 1 de julio de 1996; y de la solicitud de registro de Marca Comunitaria nº 4.482.493 "OPENBANK" (mixta).

  Open Bank Santander Consumer, S.A es también titular de esta misma marca "OPENBANK" en muchos otros países. Igualmente, es titular de los nombres de dominio <openbank.es>, <openbank.com.es>, <openbank.org>, <openbank.eu>, <openbank.co.uk>, <openbank.fr>, <openbank.nl> y <openbank.pt>.

- Openbank ha venido realizando un uso continuado de estas marcas en múltiples campañas publicitarias de productos y servicios, tanto en prensa como en radio y televisión. Además este signo y forma parte de la denominación social de esa entidad financiera y es el nombre con el que el banco es conocido en el mundo financiero y siempre en el ámbito de la telefonía y de Internet. Por ello el

público vincula la denominación "OPENBANK" con el banco y sus actividades y servicios.

- El nombre de dominio en pugna es indiscutiblemente idéntico a las marcas "OPENBANK". Esto, unido a que estas marcas son notorias en el sector financiero y ampliamente conocidas por el consumidor español, produce la confusión en el consumidor y supone un aprovechamiento indebido de la fama y prestigio adquiridos por la demandante y su marca en el mercado.
- La demandada no tiene ningún derecho ni interés legítimo respecto al nombre de dominio objeto del procedimiento y, dada la notoriedad y renombre de la marca "OPENBANK" no es creíble que su registro obedezca a un acto involuntario y casual. Además, la demandada comunicó a la demandante el registro del nombre de dominio y la posibilidad de su transferencia. A esto hay que añadir que la demandada tiene otros registrados otros muchos nombres de dominio que identifican a entidades financieras españolas muy conocidas.
- La demandada no usa el nombre de dominio objeto del procedimiento y su intención última no es otra que la apropiación del mismo para su posterior venta por una considerable cantidad o para su puesta a disposición de terceros o incluso para efectuar un fraude de phishing.

3

- Es evidente que la demandada ha registrado el nombre de dominio de mala fe ya que ella misma ha reconocido en el mensaje remitido a la demandante que no le corresponde ningún derecho sobre el mismo y que está dispuesto a transferirlo.

La demandante en su demanda solicita la transferencia del nombre de dominio <open-bank.es".

B. Demandada.

La demandada no ha contestado a la demanda.

II. Fundamentos de Derecho.

1) Reglas aplicables.

De conformidad con lo establecido en el artículo 21 del "Reglamento" el Experto Ha de resolver sobre la demanda en base a:

- las declaraciones y los documentos presentados por las partes,
- lo dispuesto en el "Plan Nacional" y en el propio "Reglamento" y
- las leyes y los principios del Derecho nacional español.

Toda la regulación del presente procedimiento de resolución extrajudicial de conflictos (el "Reglamento" y las "Normas de Procedimiento") está inspirada en el procedimiento para solución de controversias en materia de nombres de dominio del Centro de Arbitraje y Mediación de OMPI, por lo que existiendo ya una amplia Doctrina consolidada y confirmada por las Decisiones emitidas por ese Centro en materia de solución de controversias de nombres de dominio, parece razonable tomar en consideración esa Doctrina cuando los puntos examinados en esos procedimientos ante OMPI coincidan con los de la regulación española.

2) Falta de contestación a la demanda por parte de la demandada.

La demandada no ha contestado a la demanda. Por ello, el Experto debe considerar las pretensiones de la demanda teniendo en cuenta las alegaciones y la prueba aportada por la demandante. Evidentemente, el Experto no puede resolver a favor de la demandante apoyándose exclusivamente en la falta de contestación del demandado, sino que tiene que sacar las conclusiones que estime justas teniendo en cuenta las circunstancias del caso y la falta de respuesta del demandado (así se ha pronunciado la Doctrina del Centro OMPI en los Casos OMPI Nos. D2000-0277, Deutsche Bank Ag v. Giego-ArturoBruckner; D2001-1183, Bodegas Vega Sicilia, S.A. v. Serafín Rodríguez; D-2001-1479, Retevisión Móvil v. Miguel Menéndez; D2002-0908, Pans & Compañy Internacional, S.L. y Pansfood, S.A. v. Eugenio Bonilla García y D2002-1088, Transportes y Distribución, S.A. Tradisa v. Antonio Llanos Alonso).

4

Ante la falta de contestación, lo que es evidente es que la carga de la prueba recae sobre la parte demandante, pero que las pruebas aportadas por ésta no se ven alteradas por una contestación inexistente. El Experto tiene por lo tanto que decidir partiendo de las pruebas aportadas por la demandante y valorando el conjunto de circunstancias de las que tiene constancia el Experto, entre las que se encuentra el acceso a la página web con el nombre de dominio objeto de controversia (Caso OMPI No. D2001-0173, Banco Rio de la Plata, S.A. v. Alejandro Razzotti).

3) Examen de los requisitos que determinan el carácter especulativo o abusivo del nombre de dominio:

Tal y como se establece en el artículo 2 del "Reglamento" los requisitos que deben darse para que el registro del nombre de dominio tenga carácter especulativo o abusivo son:

- que el nombre de dominio sea idéntico o similar hasta el punto de crear confusión con otro término sobre el que el demandante alegue poseer derechos previos,
- que el demandado carezca de derechos o intereses legítimos sobre el nombre de dominio, y
- que el nombre de dominio haya sido registrado o utilizado de mala fe.

4) Identidad o similitud hasta el punto de causar confusión.

La demandante es titular registral del Nombre Comercial nº 209.293 "OPENBANK", solicitado el 8 de julio de 1996; de las Marcas Españolas nº 1.802.711 "OPEN BANK", nº 2.625.917 "OPENBANK" (mixta); y nº 2.656.262 "OPENBANK" (mixta), solicitada el 9 de junio de 2005; y de las Marcas Comunitarias nº 1.567.338 "OPENBANK" (mixta); nº 308.528 "OPEN BANK" (mixta), solicitada el 1 de julio de 1996; y de la solicitud de registro de Marca Comunitaria nº 4.482.493 "OPENBANK" (mixta).

Es evidente que el nombre de dominio <open-bank.es> es idéntico a las marcas y nombre comercial "OPENBANK" y "OPEN BANK" de la demandante, que han sido solicitados y concedidos con anterioridad al registro del nombre de dominio.

La única diferencia consiste en la adición del gTLD ".es" y en la introducción de un guión entre las palabras "OPEN" y "BANK". Ninguna de estas pequeñas diferencias tiene relevancia a los efectos de establecer la identidad (Casos OMPI Nº D2000-0017, Draw-Tite. Inc v. Kevin Broderick; No. D2005-1139, The Coca.Cola Compay v. Nelitalia, S.L, Nº D2002-0830 Casino Castillo de Perelada, S.A. y otros v. Montera 33, S.L.; Nº D2002-1114, Sánchez Romero Carvajal Jabugo, S.A. v. Jamones El Campo, S.L.; Nº D2001-0173 Banco Río de La Plata, S.A. v. Alejandro Razzotti; Nº D2002-0908 Pans & Company International, S.L. Pansfood, S.A. v. Eugenio Bonilla García Caso, S.L.).

Se cumple, pues, el primero de los requisitos que de acuerdo con el "Reglamento" determinan el carácter especulativo o abusivo del nombre de dominio.

5

5) Derechos e intereses legítimos sobre el nombre de dominio.

De las alegaciones y pruebas aportadas con la demanda se desprende que la demandada no tiene ninguna licencia o relación contractual con la demandante que le permita utilizar las marcas "OPENBANK" y "OPEN BANK" o aplicarla o utilizarla en cualquier nombre de domino; y en ningún momento ha recibido autorización de la demandante para registrar o utilizar el nombre de dominio <open-bank.es>.

La demandada al no contestar la demanda no ha alegado, como podía hacerlo, hechos o elementos que pudieran justificar que tuviera derechos o legítimos intereses en relación con el nombre de dominio objeto de esta controversia.

Por el contrario, la propia demandada ha venido a reconocer su falta de interés legítimo sobre el nombre de dominio en el correo electrónico enviado a la demandante y que se adjunta a la demanda en el que ofrece la transferencia del nombre de dominio objeto del procedimiento.

Así pues, hay que concluir que la demandada, según los datos que constan en el expediente, no tiene derecho o interés legítimo sobre el nombre de dominio <open-bank.es>.

6) Registro o uso del nombre de dominio de mala fe.

Como punto de partida hay que poner de manifiesto que la marca "OPENBANK" es renombrada en el mercado español, esto es, es conocida con carácter general por el gran público. Por consiguiente, hay una base sólida para considerar que la demandada, que tiene su domicilio en España, tenía perfecto conocimiento de la existencia de la marca y de su renombre al inscribir el nombre de dominio.

Puede ser además de aplicación a este caso la práctica decisoria del Centro de Mediación y Arbitraje de OMPI que mantiene que en el caso de marcas notorias o renombradas, el registro de un nombre de dominio confundible a dicha marca se considera siempre hecho de mala fe pues se presupone que cuando el demandado registra el nombre de dominio lo hace conociendo previamente la existencia de la marca[entre otros Casos OMPI D2000-0018 "Banco Español de Crédito S.A. v. Miguel Duarte Perry Vidal Tave"; D2005-1139 "The Coca-cola Company v. Netitalia, S.L"; D2000-0483 "Bankinter, S.A. v. Daniel Monclús Pérez"; y D2001-1183 "Bodegas vega Sicilia, S.A. v. Serafín Rodríguez Rodríguez".

Siendo esto así, y faltando en este caso todo interés legítimo para el registro, no parece dudoso que el registro de nombre de dominio se hizo con mala fe.

Pero es que además se dan en este caso prácticamente todos los supuestos tipificados en el artículo 2 del "Reglamento" como aquellos en los que ha de entenderse que ha existido mala fe en el registro o en el uso del nombre de dominio.

6

En primer lugar, está acreditado en el procedimiento que la demandada ha ofrecido la transferencia del nombre de dominio al demandante. En este punto, no es creíble el planteamiento de la demandada puesto de manifiesto en el correo enviado a la demandante y que consiste en presentar el registro previo del nombre de dominio como un servicio de la empresa demandada para evitar registros indeseados. Por el contrario parece evidente que la demandada registra el nombre de dominio fundamentalmente con el fin de venderlo al demandante.

A ello hay que añadir, como dato también muy significativo, que la propia demandada tiene registrados otros nombres de dominio que son marcas o identifican a otras conocidísimas entidades financieras. Tiene registrados los nombres de dominio <<banca-march.es>, <ban-caja.es>, <banco-esfinge.es>, <banco-etchevarria.es>, <banco-gallego.es>, <banco-herrero.es>, <banco-pastor.es>, <banc-sabadell.es>, <sabadell-atlantico.es>, <caja-circulo.es>, <caixa-girona.es>, caixa-penedes.es>, <caja-canarias.es>, <lloyds-bank.es>, <sol-bank.es>, <uni-caja.es>, <banco-urquijo.es>.

Son demasiadas coincidencias, que permiten considerar muy fundadamente que la demandada se ha dedicado a registrar como nombres de dominio denominaciones de empresas o entidades vinculadas al sector financiero. Una actuación de ese tipo denota la existencia de mala fe en el registro, puesto que no puede calificarse de otra manera una actuación que consiste en registrar nombres de dominio coincidentes con marcas y nombres comerciales de otras entidades con las que no se intuye que pueda tener ninguna relación el demandado (Caso OMPI Nº D-2002-1088 Transportes y Distribución, S.A Tradisa v. Antonio Llanos Alonso).

Y por último otro factor a considerar consiste en que ni el nombre de dominio objeto del presente procedimiento, esto es, <open-bank.es>, ni los otros nombres de dominio antes mencionados están activos. No parece, en efecto, razonable registrar nombres de dominio para no utilizarlos.

De todo este conjunto de circunstancias resulta indudable que la actuación de la demandada, tanto al registrar el nombre de dominio, como al no utilizarlo, es una actuación de mala fe que afecta tanto al registro del nombre de dominio como a su uso. Recuérdese que el no uso del nombre de dominio constituye una forma de uso en la medida en que se utiliza ese nombre de dominio para impedir el registro del mismo a favor del titular de la marca. Así se declaró ya desde hace tiempo, por ejemplo, en los casos OMPI Nos.D2000-0022 y D2000-0239.

Por todo ello hay que concluir que la demandada ha registrado y ha usado de mala fe el nombre de dominio <open-bank.es>.

III. Decisión.

En base a toda la fundamentación anteriormente expuesta, el Experto acuerda que el nombre de dominio <open-bank.es> sea transferido a la demandante.

_____

Alberto Bercovitz

Experto Unico

Fecha: 6 de junio de 2006

8. Ya es posible registrar dominios ".es" con los caracteres de las lenguas oficiales (novedad 2007)

http://www.red.es/prensa/notas/octubre_07/02_10_07_dominios.html

Los ".es" admiten desde el 2 de octubre símbolos como la ñ, la ç, tildes, diéresis y otros propios de las lenguas oficiales

Ya están disponibles desde el 2 de octubre los caracteres propios del castellano, catalán, euskera y gallego en el registro de dominios ".es". De este modo se cumple el compromiso adquirido por el Gobierno en la Ley de Medidas de Impulso de la Sociedad de la Información que se tramita actualmente en el Congreso de los Diputados.

Red.es, entidad del Ministerio de Industria, Turismo y Comercio que tiene asignada en España la autoridad de registro de dominios, ha informado a los Agentes Registradores Acreditados que los caracteres que podrán incorporarse a los dominios ".es" son los siguientes:

á, à , é, è , í, ï , ó, ò , ú, ü , ñ, , ç,

l•l (l geminada del catalán)

El registro de dominios ".es" con los mencionados caracteres se ha puesto en funcionamiento de forma escalonada. En una primera fase, que comenzó el 2 de octubre de 2007 a las 6:00 horas y que finalizará a las 18:00 horas del 30 de octubre de 2007, sólo los titulares de nombres de dominio registrados antes del 1 de junio de 2007 podrán solicitar la/s versión/es multilingüe/s de dichos dominios, de acuerdo con las reglas de asignación establecidas en la última instrucción y basadas en los principios de derivación y prioridad.

3. Remisión: recuerde que el dominio .eu cuenta con normativa propia

ICANN aprobó el .eu como ccTLD y abrió los registros el 7 de diciembre de 2005 para los poseedores de derechos prioritarios. El 7 de abril de 2006 se abrió el registro al público general.

Puede acceder a la misma buscando

Reglamento de la Comisión (CE) no. 874/2004 de 28 de abril de 2004, por el que se establecen normas de política de interés general relativas a la aplicación y a las funciones del dominio de primer nivel ".eu",

Cuestionario sobre Dominios

Cuestiones generales

¿A qué responde el acrónimo GTLD?

Escribe cinco de los dominios –más antiguos- de primer nivel GTLD y cuatro de los más recientes

1.
2.
3.
4.
5.

1.
2.
3.
4.

¿A qué responde el acrónimo CCTLD?

Escribe cinco de los dominios de primer nivel CCTLD.

1.
2.
3.
4.
5.

Dominios genéricos y la resolución de conflictos

Señala cuáles son las normas aplicables a la resolución de conflictos de dominios genéricos GTLD

¿Quién dictó las principales normas aplicables a la resolución de conflictos de dominios genéricos GTLD?

¿Cómo se denomina formalmente el procedimiento para la resolución de conflictos (ver párrafo 4º de la "Política"?

¿Qué entidades aplican dichas normas para la resolución de conflictos (ver párrafo 4º de la "Política"?

¿A qué responde el acrónimo OMPI?

En los procesos que se resuelven bajo la prestación de servicios de la OMPI, en principio, a quién corresponde pagar los gastos.

¿Cómo se denomina al "juez" o "jueces" encargados de resolver el conflicto?

¿Es posible reclamar en un conflicto ante la OMPI una compensación de daños y perjuicios (ver párrafo 5 de la Política??

Datos 2008

¿Alrededor de cuántos casos ha resuelto la OMPI desde 2000? ¿Cuántos casos al año resuelve?

Desde qué país se denuncia más? Y desde España

Qué país se denuncia más? Y España?

Por actividades, qué tres ambitos son los más conflictivos

¿De cada 100 demandas, en cuántas se ordena la transferencia del dominio al demandante?

De la "Política" del ICANN

El demandante en un conflicto de dominios genéricos debe demostrar tres cosas respecto del demandado (párrafo 4º), enúncielas:

1.

2.

3.

¿Basta con probar sólo una de estas tres circunstancias?

---Tengo el dominio podaderosales.com, y podaderosales.net y podaderosales.org son míos y redirigen al general podaderosales.com. Desde

hace tiempo vengo incluyendo contenidos sobre el tema y, de hecho, el índice de accesos a mi página viene extendiéndose desde hace tiempo, incluso son 34 las webs que enlazan a la mía. He sido demandado porque hay una empresa de jardinería que tiene registrada esta marca y considera que le corresponde el dominio.

Considera desde el punto de vista del párrafo 4º c), que esa empresa de jardinería tendrá derecho al nombre que yo dispongo, por qué.

Tengo el dominio podaderosales.com, y podaderosales.net y podaderosales.org son míos y redirigen al general podaderosales.com. Desde hace tiempo que creé la página y se la ofrecí a una empresa de jardinería que tenía registrada esta marca por unos 600 dólares. No me contesta y encima me ha demandado.

Considera desde el punto de vista del párrafo 4º b), que esa empresa de jardinería tendrá derecho al nombre que yo dispongo, por qué.

¿Puede la empresa de jardinería que tenía registrada esta marca (española) acudir a los tribunales españoles prescindiendo del "procedimiento administrativo"? (ver 4º k)

Si ha ido al "procedimiento administrativo" y no le han dado la razón, puede acudir a los tribunales españoles, en qué momento sería el apropiado?

Caso David Bisval

Viendo el apartado 6.4, ¿hay algún problema por que David Bisval sea una persona física y no una empresa o marca?

¿Es relevante que el demandado "·monopolizase" todos los dominios relativos a davidbisval?

¿Demuestra la mala fe el uso del dominio davidbisval vinculado a los productos de David Bisval?

Regulación del dominio .es

Dominio . es
Cuántos dominios hay aproximadamente .es??

De la evolución, te atreves a decir el motivo del significativo cambio en el último año?

Qué tipos de dominios pueden solicitarse .es??

Qué dominios requieren verificación previa?

Qué excepciones se dan al criterio de orden de llegada del dominio .es???
1
2
3
4

Normativa de dominios de 2005, extractos

Cuáles son los tres aspectos más importantes de la nueva normativa
1
2
3

Quiénes pueden solicitar un dominio.es? (legitimación)

Es posible transmitir un nombre de dominio .es, con qué requisitos?

Qué derechos confiere la asignación de un nombre de dominio?

El inclumplimiento de las obligaciones que señala el punto 13º. 5 qué consecuencias genera?

Según el punto 13º. 7, es obligatorio someterse a un sistema de resolución extrajudicial de conflictos (ver también 14. 2 c)? No es posible acudir directamente a los jueces?

Según el punto 14º el agente registrador es responsable de registrar un dominio al que no se tenga derecho o genere daños?
La decisión del sistema extrajudicial es vinculante?? Y si hay una acción judicial? (Art. 14. 2 e).

De Conflictos y Recuperación del dominio.es
Cuáles son los denominados "derechos previos":
1

2

3

Cuánto cuesta (sin contar los gastos propios de posibles abogados, etc.) recuperar un dominio .es??

Cuánto tiempo crees que cuesta recuperar un dominio.es??

En el mecanismo extrajudicial se puede obtener una indemnización, qué es lo que puede acordar el experto si estima la demanda?

Caso open-bank.es
El demandado tenía registrados más dominios bancarios? Qué método seguía para hacerlo?

El demandado se puso en contacto con Open Bank? Con qué fin.

Observa cómo openbank demuestra que tiene el nombre y la marca y los usa frecuentemente.

Sobre qué reglas se resuelve el conflicto (FJ 1º)
1.

2.

3.

Crees que las reglas del ICANN y la casuística de la OMPI para los dominios .com, .net, etc. tiene alguna relevancia para la resolución de conflictos .es??

Qué significado jurídico tiene la no contestación a la demanda).

Qué tres cosas tiene que demostrar la parte demandante (openbank)
En concreto, cómo estima el árbitro que se da mala fe??
1.
2.
3.

¿Desde cuándo es posible registrar dominios .es con caracteres como ñ, o Ç?

¿Desde cuándo está en marcha el dominio .eu?

¿Qué norma básica he de tener en cuenta para las cuestiones de dominios .eu?

XIV. ADMINISTRACIÓN ELECTRÓNICA , LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS.

(téngase en cuenta, entre otros, lo afirmado sobre protección de datos y Administración y firma electrónica y Administración).

Asimismo, aunque excede lo exigible a este curso, téngase en cuenta:

Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio, con relación al fenómeno electrónico y especialmente la e-Administración

Esquema Nacional de Interoperabilidad, regulado por Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Esquema Nacional de Seguridad, regulado por Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica el desarrollo reglamentario de la Ley

Asimismo, son ya diversas las normas autonónicas de e-Administración, incluso normas legales, como la Ley 3/2010, de 5 de mayo, de la Generalitat, de administración electrónica de la Comunitat Valenciana.

1. Elementos generales

ANEXO

Definiciones

A efectos de la presente ley, se entiende por:

a) Actuación administrativa automatizada: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

d) Autenticación: Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos, y de la integridad y autoría de estos últimos.

e) Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc).

h) Ciudadano: Cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas.

j) Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

k) Estándar abierto: Aquel que reúna las siguientes condiciones:

- sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

- su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

o) Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

p) Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

TÍTULO PRELIMINAR

Del ámbito de aplicación y los principios generales

Artículo 4. Principios generales.

La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios:

b) Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos, tanto respecto al acceso a la prestación de servicios públicos como respecto a cualquier actuación o procedimiento administrativo sin perjuicio de las medidas dirigidas a incentivar la utilización de los medios electrónicos.

d) Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

h) Principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos.

i) Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

j) Principio de simplificación administrativa, por el cual se reduzcan de manera sustancial los tiempos y plazos de los procedimientos administrativos, logrando una mayor eficacia y eficiencia en la actividad administrativa.

k) Principio de transparencia y publicidad del procedimiento, por el cual el uso de medios electrónicos debe facilitar la máxima difusión, publicidad y transparencia de las actuaciones administrativas.

Artículo 34. Criterios para la gestión electrónica.

La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación.

b) La previsión de medios e instrumentos de participación, transparencia e información.

c) La reducción de los plazos y tiempos de respuesta.

d) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas.

2. Derecho a relacionarse con las Administraciones Públicas

TÍTULO PRIMERO

Derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos

Artículo 6. Derechos de los ciudadanos.

1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 27. Comunicaciones electrónicas.

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.

2. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.

3. Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

4. Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas.

5. Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.

6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

7. Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes.

Artículo 8. Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos.

1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

2. La Administración General del Estado garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

a) Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Puntos de acceso electrónico, consistentes en sedes electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

c) Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

Disposición final séptima. Desarrollo reglamentario del artículo 4.c).

El Gobierno desarrollará reglamentariamente lo previsto en el artículo 4.c) de la presente Ley para garantizar que todos los ciudadanos, con especial atención a las personas con algún tipo de discapacidad y mayores, que se relacionan con la Administración General del Estado puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos.

3. Derechos del artículo 6. 2º

(art. 6)

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.

c) A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.

f) A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.

i) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

j) A la calidad de los servicios públicos prestados por medios electrónicos.

k) A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

3. En particular, en los procedimientos relativos al establecimiento de actividades de servicios, los ciudadanos tienen derecho a obtener la siguiente información a través de medios electrónicos:

a) Los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.

b) Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como de las asociaciones y organizaciones profesionales relacionadas con las mismas.

c) Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios y las vías de recurso en caso de litigio entre cualesquiera autoridades competentes, prestadores y destinatarios.

Derecho a no aportar datos… (arts. 6. 2. b) y 9).

Art. 6. 2º b) Derecho a …

b) A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.

Artículo 9. Transmisiones de datos entre Administraciones Públicas.

1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a

los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley.

Garantía e implantación de los derechos…

Artículo 7. Defensa de los derechos de los ciudadanos.

1. En la Administración General del Estado, se crea la figura del Defensor del usuario de la administración electrónica, que velará por la garantía de los derechos reconocidos a los ciudadanos en la presente Ley, sin perjuicio de las competencias atribuidas en este ámbito a otros órganos o entidades de derecho público. Será nombrado por el Consejo de Ministros a propuesta del Ministro de Administraciones Públicas entre personas de reconocido prestigio en la materia. Estará integrado en el Ministerio de Administraciones Públicas y desarrollará sus funciones con imparcialidad e independencia funcional.

2. El Defensor del usuario de la administración electrónica elaborará, con carácter anual, un informe que se elevará al Consejo de Ministros y se remitirá al Congreso de los Diputados. Dicho informe contendrá un análisis de las quejas y sugerencia recibidas así como la propuesta de las actuaciones y medidas a adoptar en relación con lo previsto en el apartado 1 de este artículo.

3. Para el ejercicio de sus funciones, el Defensor del usuario de la administración electrónica contará con los recursos de la Administración General del Estado con la asistencia que, a tal efecto, le presten las Inspecciones Generales de los Servicios de los Departamentos ministeriales y la Inspección General de Servicios de la Administración Pública. En particular, las Inspecciones de los Servicios le asistirán en la elaboración del informe al que se refiere el apartado anterior y le mantendrán permanentemente informado de las quejas y sugerencias que se reciban en relación con la prestación de servicios públicos a través de medios electrónicos. A estos efectos, la Comisión Coordinadora de las Inspecciones generales de servicios de los departamentos ministeriales realizará, en este ámbito, las funciones de coordinación que tiene legalmente encomendadas.

4. Reglamentariamente se determinará el estatuto del Defensor del usuario de la administración electrónica, así como la regulación de sus relaciones con los órganos a los que se refiere el apartado anterior de este artículo.

Disposición final tercera. Adaptación de las Administraciones Públicas para el ejercicio de derechos.

1. Desde la fecha de entrada en vigor de la presente Ley, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con los procedimientos y actuaciones adaptados a lo dispuesto en la misma, sin perjuicio de lo señalado en los siguientes apartados. A estos efectos, cada Administración Pública hará pública y mantendrá actualizada la relación de dichos procedimientos y actuaciones.

2. En el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009. A tal fin, el Consejo de Ministros establecerá y hará público un calendario de adaptación gradual de aquellos procedimientos y actuaciones que lo requieran.

3. En el ámbito de las Comunidades Autónomas, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias.

4. En el ámbito de las Entidades que integran la Administración Local, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias. A estos efectos las Diputaciones Provinciales, o en su caso los Cabildos y Consejos Insulares u otros organismos supramunicipales, podrán prestar los servicios precisos para garantizar tal efectividad en el ámbito de los municipios que no dispongan de los medios técnicos y organizativos necesarios para prestarlos.

4. De la sede electrónica y publicaciones electrónicas

TÍTULO SEGUNDO

Régimen jurídico de la administración electrónica

CAPÍTULO I

De la sede electrónica

Artículo 10. La sede electrónica.

1. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Artículo 11. Publicaciones electrónicas de Boletines Oficiales.

1. La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.

2. La publicación del «Boletín Oficial del Estado» en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

Disposición final segunda. Publicación electrónica del «Boletín Oficial del Estado».

La publicación electrónica del «Boletín Oficial del Estado» tendrá el carácter y los efectos previstos en el artículo 11.2 de la presente Ley desde el 1 de enero de 2009.

Nota ejemlo Comunidad Valenciana: Por Decreto 183/2006, de 15 de diciembre, del Consell (de la Generalitat Valenciana) se establece que el Diari Oficial se publicará en formato electrónico, como única versión, oficial y autentica, quedando garantizada la identificación del titular competente para su publicación, y de la voluntad de la publicación del Diari Oficial, a través de la firma electrónica del documento por parte del mismo.

Art. 1. 2º "El Diari Oficial está integrado por un conjunto de documentos electrónicos, firmados, verificados y autentificados individualmente de forma electrónica, de acuerdo con las normas de la Autoritat de Certificació de la Comunitat Valenciana (ACCV). Estos documentos tienen la consideración de únicos documentos originales y serán custodiados y conservados por la Autoritat de Certificació de la Comunitat Valenciana."

Art. 4 "El Diari Oficial de la Comunitat Valenciana se publicará en formato electrónico, como única versión, que tendrá la consideración de oficial y autentica. …

El Diari Oficial de la Comunitat Valenciana se podrá editar también en otros formatos físicos (microficha, etc.) y en cualquier soporte informático, actual y futuro, que

permita su mayor difusión y mejora del servicio. *Excepcionalmente* se podrá difundir en soporte papel, cuya tirada se determinará por el director general de Relaciones con las Cortes y Secretariado del Gobierno, de la Presidencia de la Generalitat."

Artículo 12. Publicación electrónica del tablón de anuncios o edictos.

La publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente.

5. Registros y plazos

CAPÍTULO III .

De los registros, las comunicaciones y las notificaciones electrónicas

Sección 1.ª De los Registros

Artículo 24. Registros electrónicos.

1. Las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Artículo 25. Creación y funcionamiento.

1. Las disposiciones de creación de registros electrónicos se publicarán en el Diario Oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles a los efectos previstos en el artículo siguiente.

Art. 24

2. Los registros electrónicos podrán admitir:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

Art. 24. 2 b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

Art. 25. 2º. En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones a las que se refiere el apartado

2.a) que pueden presentarse en el mismo así como, en su caso, la posibilidad de presentación de solicitudes, escritos y comunicaciones a los que se refiere el apartado 2.b) de dicho artículo.

(Artículo 35. Iniciación del procedimiento por medios electrónicos.)

2. Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos.

Art. 24…

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

4. En el ámbito de la Administración General del Estado se automatizarán las oficinas de registro físicas a las que se refiere el artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a fin de garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Artículo 25. Creación y funcionamiento.

…

…

3. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

4. Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.

Artículo 26. Cómputo de plazos.

1. Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las Administraciones Públicas por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.

2. Los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas.

3. A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

5. Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. En todo caso, no será de aplicación a los registros electrónicos lo dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

(5. Cuando un día fuese hábil en el municipio o Comunidad Autónoma en que residiese el interesado, e inhábil en la sede del órgano administrativo, o a la inversa, se considerará inhábil en todo caso.)

27 (ya reproducido).

6. Notificación

Artículo 28. Práctica de la notificación por medios electrónicos.

1. Para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización, sin perjuicio de lo dispuesto en el artículo 27.6. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados anteriormente podrán emitirse y recabarse, en todo caso, por medios electrónicos.

2. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

3. Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido

rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992 de Régimen Jurídico y del Procedimiento Administrativo Común y normas concordantes, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

4. Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de Régimen Jurídico y del Procedimiento Administrativo Común, excepto en los casos previstos en el artículo 27.6 de la presente Ley.

5. Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dichos acceso.

YA VISTO Artículo 32. Expediente electrónico.

1. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

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

7. Procedimiento gestionado de forma electrónica

TÍTULO TERCERO

De la gestión electrónica de los procedimientos

CAPÍTULO I

Disposiciones comunes

Artículo 33. Utilización de medios electrónicos.

1. La gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa.

2. En la aplicación de medios electrónicos a la actividad administrativa se considerará la adecuada dotación de recursos y medios materiales al personal que vaya a utilizarlos, así como la necesaria formación acerca de su utilización.

Artículo 34 (ya reproducido)

CAPÍTULO II

Utilización de medios electrónicos en la tramitación del procedimiento

Artículo 35. Iniciación del procedimiento por medios electrónicos.

1. La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado i) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos.

3. Con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

Artículo 36. Instrucción del procedimiento utilizando medios electrónicos.

1. Las aplicaciones y sistemas de información utilizados para la instrucción por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación de los órganos responsables de los procedimientos así como la tramitación ordenada de los expedientes y facilitar la simplificación y la publicidad de los procedimientos.

2. Los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre los órganos y unidades intervinientes a efectos de emisión y recepción de informes u otras actuaciones deberán cumplir los requisitos establecidos en esta Ley.

3. Cuando se utilicen medios electrónicos para la participación de los interesados en la instrucción del procedimiento a los efectos del ejercicio de su derecho a presentar alegaciones en cualquier momento anterior a la propuesta de resolución o en la práctica del trámite de audiencia cuando proceda, se emplearán los medios de comunicación y notificación previstos en los artículos 27 y 28 de esta Ley.

Art. 6. 2.

d) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.

e) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.

Artículo 37. Acceso de los interesados a la información sobre el estado de tramitación.

1. En los procedimientos administrativos gestionados en su totalidad electrónicamente, el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido donde éste pueda consultar, previa identificación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.

2. En el resto de los procedimientos se habilitarán igualmente servicios electrónicos de información del estado de la tramitación que comprendan, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable.

Artículo 38. Terminación de los procedimientos por medios electrónicos.

1. La resolución de un procedimiento utilizando medios electrónicos garantizará la identidad del órgano competente mediante el empleo de alguno de los instrumentos previstos en los artículos 18 y 19 de esta Ley.

2. Podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto.

Artículo 39. Actuación administrativa automatizada.

En caso de actuación automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

8. Cooperación

TÍTULO CUARTO

Cooperación entre administraciones para el impulso de la administración electrónica

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 40. Comité Sectorial de administración electrónica.

1. El Comité Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General del Estado, de las administraciones de las Comunidades Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica.

2. El Comité Sectorial de la administración electrónica velará por el cumplimiento de los fines y principios establecidos en esta Ley, y en particular desarrollará las. siguientes funciones:

a) Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.

b) Preparar planes programas conjuntos de actuación para impulsar el desarrollo de la administración electrónica en España.

3. Cuando por razón de las materias tratadas resulte de interés podrá invitarse a las organizaciones, corporaciones o agentes sociales que se estime conveniente en cada caso a participar en las deliberaciones del comité sectorial.

CAPÍTULO II

Cooperación en materia de interoperabilidad de sistemas y aplicaciones

Artículo 41. Interoperabilidad de los Sistemas de Información.

Las Administraciones Públicas utilizarán las tecnologías de la información en sus relaciones con las demás administraciones y con los ciudadanos, aplicando medidas informáticas, tecnológicas, organizativas, y de seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 42. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

1. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

4. En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos

efectos considerarán la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

Artículo 43. Red de comunicaciones de las Administraciones Públicas españolas.

La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

Artículo 44. Red integrada de Atención al Ciudadano.

1. Las Administraciones Públicas podrán suscribir convenios de colaboración con objeto de articular medidas e instrumentos de colaboración para la implantación coordinada y normalizada de una red de espacios comunes o ventanillas únicas.

2. En particular, y de conformidad con lo dispuesto en el apartado anterior, se implantarán espacios comunes o ventanillas únicas para obtener la información prevista en el artículo 6.3 de esta Ley y para realizar los trámites y procedimientos a los que hace referencia el apartado a) de dicho artículo.

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías

Artículo 45. Reutilización de sistemas y aplicaciones de propiedad de la Administración.

1. Las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier Administración sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente la incorporación de los ciudadanos a la Sociedad de la información

Artículo 46. Transferencia de tecnología entre Administraciones.

1. Las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo de la administración electrónica y de conformidad con lo que al respecto se establezca en el Esquema Nacional de Interoperabilidad.

2. La Administración General del Estado, a través de un centro para la transferencia de la tecnología, mantendrá un directorio general de aplicaciones para su reutilización, prestará asistencia técnica para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes de especial interés para el desarrollo de la administración electrónica en el marco de los esquemas nacionales de interoperabilidad y seguridad.

9. Lenguas

…

Disposición adicional sexta. Uso de Lenguas Oficiales.

1. Se garantizará el uso de las lenguas oficiales del Estado en las relaciones por medios electrónicos de los ciudadanos con las Administraciones Públicas, en los términos previstos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en la normativa que en cada caso resulte de aplicación.

2. A estos efectos, las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

3. Los sistemas y aplicaciones utilizados en la gestión electrónica de los procedimientos se adaptarán a lo dispuesto en cuanto al uso de lenguas cooficiales en el artículo 36 de la ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común.

4. Cada Administración Pública afectada determinará el calendario para el cumplimiento progresivo de lo previsto en la presente disposición, debiendo garantizar su cumplimiento total en los plazos establecidos en la disposición final tercera.

Cuestionario sobre Ley 11/2007 sobre administración electrónica

Elementos generales

Qué significa para la Ley 11/2007 un "medio electrónico" (anexo).

A la vista del principio de igualdad del artículo 4 b), crees que es posible establecer diferencias entre los administrados electrónicamente y los que sólo lo hacen por medios no virtuales? Se te ocurre algún trato diferente?

A la vista del principio de legalidad del artículo 4 d), en principio, crees que es necesaria una ley para establecer alguna diferencia para la relación electrónica en las garantías de la ley 30/1992?

A la vista del principio de calidad de la información del artículo 4 h), crees que la Administración –en principio- puede eximirse de responsabilidad por la información administrativa de sus páginas web?

Sigue el principio de simplificación administrativa del art. 4 i) y lee los criterios para la gestión electrónica (art. 34). Resume qué aspectos esenciales deben estudiarse previamente para la aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios:

1.

2.

3.

4.

Derecho a relacionarse con las Administraciones Públicas

Observa el artículo 6. 1º. Se te ocurre alguna finalidad para la que no se reconozca la posibilidad de relacionarse electrónicamente con la administración?

A la vista del artículo 27:

Es posible excepcionar el derecho a la relación electrónica. Qué exige el artículo 27. 1º para que la relación sea sólo por medio no electrónico?

Puede un ciudadano pasar de un canal electrónico a uno no electrónico y viceversa en mitad de un procedimiento, cuando quiera? Tiene que justificar su cambio? (art. 27 .1º).

A la vista del artículo 6. 1º y del 27. 2º crees que en principio puede obligarse a la relación electrónica al ciudadano. Lee el artículo 27. 6º. Es necesaria la ley para obligar a la relación electrónica?

Qué criterios tiene la ley (art. 27. 6º) para que se pueda obligar a la relación electrónica? Se te ocurre algún ejemplo que te resulte razonable que se pueda obligar a la relación electrónica?

Cómo puede saber el ciudadano los medios electrónicos que puede usar para ejercer la relación electrónica (art. 27. 4º).

Qué relación crees que tiene el artículo 8. 1º con el derecho del artículo 6. 1º?

Que tres canales son obligatorios para la Administración General del Estado (art. 8. 2º).

1.

2.

3.

Derechos del artículo 6. 2º

Crees que se te puede tratar de forma diferente por utilizar un navegador u otro a la hora de relacionarte electrónicamente con la Administración? (art. 6. 2. c).

Tengo derecho a poder utilizar con la Administración cualquier software que utilice estándares abiertos? (art. 6. 2 k). Es posible que la Administración no permita la relación electrónica a través de software de estándar abierto, en qué caso?

Derecho a no aportar datos… (arts. 6. 2. b) y 9).

En principio, tengo derecho a no aportar al Ayuntamiento de Valencia información o documentos que ya obran en su poder?

En principio, tengo derecho a no aportar al Ayuntamiento de Valencia información o documentos que obran en poder de la Generalitat?

Voy a pedir una ayuda al Ayuntamiento y necesitan mi declaración de renta. ¿es posible que me niegue a que el Ayuntamiento acceda a esta información de la Agencia Tributaria estatal?

Si en el caso anterior he dado mi consentimiento al Ayuntamiento, está obligada la Agencia Tributaria a facilitar la declaración de renta? (observe cómo

se hace referencia al término "Acceso" y no "comunicación" o "cesión" de datos.

Voy a pedir una licencia de un bar al Ayuntamiento. La normativa que regula esa licencia no exige información sobre mi declaración de renta. El Ayuntamiento puede solicitar el acceso a esa información a la Agencia Tributaria?

Garantía e implantación de los derechos…

Cómo se llama la figura que "velará por la garantía de los derechos reconocidos a los ciudadanos en la presente Ley" (art. 7). Para qué Administración es?

Lea la *Disposición final tercera.…*

En qué fecha obligatoriamente la Administración General del Estado deberá hacer efectivos los derechos del artículo 6?

Crees que los Ayuntamientos y las Comunidades Autónomas están realmente obligadas a hacer efectivos los derechos del art. 6?

Sede electrónica

Qué es una sede electrónica? Se te ocurre un ejemplo? Art. 10.

Qué debe garantizarse "en todo caso" en una sede electrónica. Qué principios deben regir la creación de una sede electrónica? (art. 10. 3º)

Crees en razón del artículo 11. 1º que el diario oficial de una Comunidad Autónoma necesariamente ha de considerarse como oficial y auténtico.

Crees posible que un diario oficial se publique sólo con carácter auténtico en su versión de internet, no en papel?

Respecto del Diari Oficial de la Comunitat Valenciana, se prevé su publicación en papel, con qué carácter?

Es posible que las publicaciones obligatorias en edictos o anuncios se hagan sólo en la sede electrónica?

Registros

Es obligatoria la creación de un registro para las Administraciones Públicas? (art. 24).

Qué han de regular obligatoriamente las disposiciones de creación de registros electrónicos:

1

2

3

Cómo puedo saber qué tipos de instancias puedo presentar a cada administración? (art. 25. 2).

A la vista del artículo 24. 2 b) y 24. 3º crees posible que se obligue en general al ciudadano a utilizar únicamente el formulario preestablecido para usarlo en el registro electrónico?

A la vista del artículo 24. 4º crees que puedo utilizar el registro electrónico del Ministerio de Hacienda para remitir un escrito dirigido al Ministerio de Trabajo.

A la vista del artículo 24. 3º crees que puedo utilizar el registro electrónico del Ministerio de Hacienda para remitir un escrito dirigido a la Generalitat Valenciana? En qué caso sí sería posible.

Cómo tengo seguridad de que he registrado algo en el registro electrónico (art. 25. 3º).

Puedo aportar documentos con mi solicitud en el registro electrónico (por ejemplo, un documento pdf. firmado electrónicamente sobre la concesión de una licencia), con qué requisitos (art. 25. 4º).

Plazos

Puedo registrar electrónicamente a las 4 horas de la madrugada? (Art. 26. 1).

Si presento a las 4 h de un domingo, en qué momento se considerará que he hecho el registro (art. 26.3º)?

En qué momento crees que se cumplirá con la comunicación a la que se refiere el artículo 26. 4º -final- (ver art. 25.3º).

Uso internet en Valencia en día festivo de fallas para registrar un escrito dirigido a la Junta de Andalucía, en día que es laborable. Quién señala qué días son inhábiles? (Art. 26. 5º)

Notificación electrónica

En principio, me pueden notificar electrónicamente sin que yo lo haya solicitado (art. 28. 1º)?

Crees posible que sin haber consentido en ser notificado electrónicamente, me puedan notificar válidamente (art. 28. 1º). Imagina un supuesto de recepción de un mail en el que me señalan que se trata de una notificación en un procedimiento.

Es posible que cambie de posición y decida que no me notifiquen electrónicamente? (art. 28. 4º), tengo que justificar esta decisión?

Cuándo se entiende que una notificación electrónica ha sido rechazada (art. 28. 3º)

A la vista de la noción "puesta a disposición" (art. 28. 3º) o del artículo 28. 5º, qué formas se te ocurren de notificación que sean diferentes de recibir un correo electrónico?

Otros

Acceso al estado de tramitación: lea conjuntamente el artículo 6. 2. d) y el art. 37. Si el procedimiento no se tramita electrónicamente en su totalidad, tengo derecho a conocer el estado de tramitación electrónicamente? (art. 37. 1º).

Si el procedimiento se tramita electrónicamente en su integridad, qué mínimo de información garantiza el artículo 37. 2º?

Es posible que se dicten resoluciones administrativas automatizadas (art. 38. 2 y 30?

Como se llama al "conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad" (art. 42).

Cómo se aprueba lo referido en el artículo 42?

Lengua en la e-administración

Cuándo se debe garantizar que los contenidos estén en lenguas cooficiales? (Disposición adicional sexta, apt. 2ºº)

XV. FIRMA ELECTRÓNICA EN GENERAL Y EN LA ADMINISTRACIÓN

Ley de Enjuiciamiento Civil, documento y firma electrónica

Artículo 267. Forma de presentación de los documentos públicos.

Cuando sean públicos los documentos que hayan de aportarse conforme a lo dispuesto en el artículo 265, podrán presentarse por copia simple, ya sea en soporte papel o, en su caso, en soporte electrónico a través de imagen digitalizada incorporada como anexo que habrá de ir firmado mediante firma electrónica reconocida y, si se impugnara su autenticidad, podrá llevarse a los autos original, copia o certificación del documento con los requisitos necesarios para que surta sus efectos probatorios.

Artículo 268. Forma de presentación de los documentos privados.

1. Los documentos privados que hayan de aportarse se presentarán en original o mediante copia autenticada por el fedatario público competente y se unirán a los autos o se dejará testimonio de ellos, con devolución de los originales o copias fehacientes presentadas, si así lo solicitan los interesados. Estos documentos podrán ser también presentados mediante imágenes digitalizadas, incorporadas a anexos firmados electrónicamente.

2. Si la parte sólo posee copia simple del documento privado, podrá presentar ésta, ya sea en soporte papel o mediante imagen digitalizada en la forma descrita en el apartado anterior, que surtirá los mismos efectos que el original, siempre que la conformidad de aquélla con éste no sea cuestionada por cualquiera de las demás partes.

3. En el caso de que el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, se presentará copia auténtica o se designará el archivo, protocolo o registro, según lo dispuesto en el apartado 2 del artículo 265.

Artículo 326. Fuerza probatoria de los documentos privados.

1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.

2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.

Ley 59/2003, de 19 de diciembre, de firma electrónica

…

TITULO I

Disposiciones generales

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La 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.

2. La 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.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Nuevo LMISI

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.»

6. El documento electrónico será soporte de.

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o

administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

NUEVO LMISI

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

Artículo 5. Régimen de prestación de los servicios de certificación.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

TITULO II

Certificados electrónicos

CAPITULO I

Disposiciones generales

Artículo 6. Concepto de certificado electrónico y de firmante.

1. Un certificado electrónico es un 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.

2. El firmante es 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.

...

CAPITULO II

Certificados reconocidos

Artículo 11. Concepto y contenido de los certificados reconocidos.

1. Son 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.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

...

Información sobre prestadores de servicios de certificación

Prestadores servicios de cerfitifcación (noviembre 2007)

https://www11.mityc.es/prestadores

En virtud de la Ley 59/2003, de 19 de diciembre, de firma electrónica artículo 30, y disposición transitoria segunda,

Servicios de certificación basados en certificados reconocidos

Prestadores

Servicios de certificación basados en certificados reconocidos

Prestadores

AC ABOGACÍA

ANCERT - Agencia Notarial de Certificación

ANF AC

Autoritat de Certificació de la Comunitat Valenciana - ACCV

BANESTO CA

CAMERFIRMA

CATCert

CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)

CICCP

Dirección General de la Policía

FIRMAPROFESIONAL

Izenpe, S.A

Servicios de validación temporal

Prestadores

Autoritat de Certificació de la Comunitat Valenciana - ACCV

CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)

e-firma en la Administración. Documentos electrónicos (Ley firma 53/2003 y Ley e-Administración 11/2006)

Ley 53/2003 de e-firma y Administración

Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por 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.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo

informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

…

Artículo 15. Documento nacional de identidad electrónico.

1. El 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.

2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. Requisitos y características del documento nacional de identidad electrónico.

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

Ley 11/2007 de administración electrónica y autenticación, acreditación y firma

TÍTULO PRIMERO. **Derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos**

Artículo 6. Derechos de los ciudadanos.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

g) A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.

h) A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.

Artículo 27. Comunicaciones electrónicas.

3. Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

CAPÍTULO II

De la identificación y autenticación

Sección 1.ª Disposiciones comunes

Artículo 13. Formas de identificación y autenticación.

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.

b) Sistemas de firma electrónica para la actuación administrativa automatizada.

c) Firma electrónica del personal al servicio de las Administraciones Públicas.

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

Sección 2.ª Identificación de los ciudadanos y autenticación de su actuación

Artículo 14. Utilización del Documento Nacional de Identidad.

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

Artículo 4. Principios generales.

g) Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

Artículo 15. Utilización de sistemas de firma electrónica avanzada.

1. Los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, referidos en el artículo 14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

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

3. Los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen.

Artículo 16. Utilización de otros sistemas de firma electrónica.

1. Las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.

2. En aquellos supuestos en los que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública, ésta deberá garantizar la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos.

3. Cuando resulte preciso, las Administraciones Públicas certificarán la existencia y contenido de las actuaciones de los ciudadanos en las que se hayan usado formas de identificación y autenticación a que se refiere este artículo.

Sección 3.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 17. Identificación de las sedes electrónicas.

Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.

Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Los certificados electrónicos a los que se hace referencia en el apartado 1.a) incluirán el número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

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

Artículo 19. Firma electrónica del personal al servicio de las Administraciones Públicas.

1. Sin perjuicio de lo previsto en los artículos 17 y 18, la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados.

2. Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. La firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse a los efectos de este artículo.

Artículo 20. Intercambio electrónico de datos en entornos cerrados de comunicación.

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos y entidades de derecho público,

serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo.

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

3. Cuando los participantes pertenezcan a distintas administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Sección 4.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos

Artículo 21. Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos.

1. Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

2. Los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.

3. La Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones. Cada Administración Pública podrá disponer de los mecanismos necesarios para la verificación del estado de revocación y la firma con los certificados electrónicos admitidos en su ámbito de competencia.

Artículo 22. Identificación y autenticación de los ciudadanos por funcionario público.

1. En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 13 de los que aquel no disponga, tal identificación o autenticación podrá ser validamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

2. Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

3. Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación regulada en este artículo.

Artículo 23. Formas de Representación.

Sin perjuicio de lo dispuesto en el artículo 13.2, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación.

Documento, archivo y expediente electrónicos en la Administración. "Copias" y derecho a las copias

Ley 30/1992 documento

Ley 30/1992

Artículo 45. Incorporación de medios técnicos.

...

5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes.

Artículo 46. Validez y eficacia de documentos y copias.

1. Cada Administración Pública determinará reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos o privados.

2. Las copias de cualesquiera documentos públicos gozarán de la misma validez y eficacia que estos siempre que exista constancia de que sean auténticas.

3. Las copias de documentos privados tendrán validez y eficacia, exclusivamente en el ámbito de la actividad de las Administraciones Públicas, siempre que su autenticidad haya sido comprobada.

4. Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas.

Definición de "documento electrónico" en Anexo de la Ley 11/2007

j) Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Ley 11/2007

CAPÍTULO IV

De los documentos y los archivos electrónicos

Artículo 29. Documento administrativo electrónico.

1. Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección 3.ª del Capítulo II de la presente Ley.

2. Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

3. La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

(ejemplos importancia del tiempo) arts. 26 y 27.

Artículo 26. Cómputo de plazos.

4. El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

Artículo 28. Práctica de la notificación por medios electrónicos.

2. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

Artículo 30. Copias electrónicas.

1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

2. Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

5. Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Art. 6. 2. Se reconoce el derecho a…

e) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.

Artículo 31. Archivo electrónico de documentos.

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

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

Artículo 32. Expediente electrónico.

1. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

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

Cuestionario sobre Firma electrónica

En la regulación de la Ley de enjuiciamiento civil, sobre la presentación de documentos…

¿se puede presentar una copia del documento público original escaneada y firmada digitalmente?

¿y si la parte contraria no se fía de esa copia presentada y firmada electrónicamente, qué sucede?

¿Crees que si la firma electrónica reconocida es válida, ello quiere decir que el documento público que se ha presentado así en copia necesariamente será prueba válida?

Crees que es una prueba que surte todos los efectos un documento electrónico firmado con firma reconocida por un notario.

¿Los documentos privados tienen que prestarse con firma electrónica reconocida?

Ley de firma electrónica

¿Como se define la firma electrónica? (art. 3)

¿Y la firma electrónica avanzada?

Qué es "firma electrónica reconocida"

Qué valor jurídico se le otorga a la firma electrónica reconocida (art. 3. 4º). Si se impugna en juicio la autenticidad de la firma electrónica reconocida, qué es lo único que cabe comprobar? (art. 3. 8º).

Qué es un documento electrónico (art. 3. 5). Puede ser un documento privado "documento electrónico"

Si no es firma electrónica reconocida, ¿no tiene valor jurídico de prueba? (art. 3. 9).

He bajado un programa libre de internet de firma electrónica, lo utilizo y he realizado una compraventa ayudándome de dicha herramienta para las comunicaciones con el vendedor. Sin embargo, ahora el vendedor niega que hayamos acordado la compraventa:

¿puedo utilizar las pruebas de nuestras comunicaciones como prueba en un juicio? Y si no hubiera utilizado tan siquiera dicha firma electrónica.

Entre partes (por ejemplo, relaciones de contratación frecuentes con una entidad) se puede haber pactado el valor que se otorga a una firma electrónica determinada? (art. 3. 10º).

Qué es un certificado electrónico? (art. 6)

Qué es un certificado electrónico reconocido? (art. 7)

Escribe 5 de los prestadores de servicios de certificación, certificados reconocidos

1

2

3

4

5

General e-firma

e-firma en la Administración

Qué es el DNI electrónico (art. 15 Ley firma)

Sólo están obligadas a reconocer el e-DNI las administraciones? (art.15. 2º)

A la vista del artículo 16, qué tipo de firma viene a ser el e-DNI?

Ley 11/2007 de administración electrónica y firma (arts. 13 y ss.)

Qué se exige para la validez de las comunicaciones electrónicas (art. 27. 3º)?

Todos los que tengan e-DNI tienen derecho a usarlo con cualquier Administración? (art. 6 y art. 13. 2 a) y º4).

Tenemos derecho a usar otros sistemas de firma electrónica con las Administraciones Públicas?

Todos los sistemas de firma electrónica de los que habla el artículo 13. 2º o el art. 15.1 son firma avanzada? (art. 16).

En razón del artículo 15. 2º crees que cada Administración determina el sistema de firma que admite? Qué deben hacer para que los administrados lo sepan?

Ten en cuenta el artículo 4, g). Qué crees que significa este principio para que las administraciones elijan el sistema de acreditación de identidad y autenticación. Siempre será exigible la firma electrónica basada en certificado reconocido, o cuanto menos la firma avanzada?

Para qué crees que es necesario que una sede electrónica de una Administración use un sistema de firma electrónica?

Cuando la Administración actúa de forma automatizada que dos sistemas de identificación y autentificación puede utilizar (art. 18. 1º)

Crees que un funcionario que actúe electrónicamente puede identificarse con su propio e-DNI? Crees que es posible que se identifique electrónicamente de otra manera? Cómo? (art. 19).

En general las Administraciones Públicas entre ellas deben aceptar como válidos todos los certificados electrónicos "reconocidos"? (art. 21). Crees que es posible que entre ellas acepten otros sistemas de firma no "reconocidos" (art. 21. 2º).

Un ciudadano que no tenga firma electrónica, crees que puede hacer alguna actuación electrónica con la Administración que precise de firma electrónica, cómo? (art. 22).

Crees posible que haya "gestores" que realicen en nuestro nombre actuaciones con firma electrónica con la administración? (art. 23).

Documento electrónico en la administración electrónica

Ley 30/1992

Qué requisitos exige en general el artículo 45. 5º para la validez de los documentos en soportes electrónicos.

Qué exige el artículo 46 para la validez de las copias de los documentos?

Firma en Ley 11/2007

Observa el artículo 4. 1º de la Ley 59/2003 de firma, respecto de la administración y fija la atención en el requisito del artículo 29. 2º de la Ley 11/2007. De qué requisito se trata? Es necesario siempre que se acredite por procedimientos de firma? (recuerda el principio de proporcionalidad).

A la vista del artículo 26. 4, qué importancia puede tener que se sepa a qué hora se ha registrado un escrito, solicitud o comunicación?

Vuelve a la lista de "Información sobre prestadores de servicios de certificación" quienes son prestadores de servicios de sellado de tiempo?

Fija tu atención en la definición de "documento electrónico" (anexo). Luego fija la atención en la noción de "copia electrónica" (art. 30). Luego, observa la referencia del artículo 29 a "manteniéndose o no el formato original". ¿Se te ocurre por qué se dice eso? Piensa en cómo se puede "emitir" un documento electrónico y si lo normal será que pase a ser una "copia" de la información electrónica.

Es posible que la Administración pase el documento electrónico a documento de papel? Con qué requisitos para que sean copias auténticas ¿ (art. 30. 5º)

Es posible que la Administración digitalice sus propios documentos y luego destruya los originales de papel (art. 30.4º)?

Es posible que la Administración digitalice documentos de los ciudadanos y pasen a tener plena validez y eficacia (art. 30.3º)?

A la vista del derecho del art. 6. 2 a) y del significado de documento y copia electrónica, crees que sería posible reconocer el derecho a acceder al documento electrónico? Se te ocurre un ejemplo de cómo se haría posible el derecho a obtener una copia electrónica?

Qué es el expediente electrónico? (Art. 32)

Cómo debe foliarse el conjunto de documentos electrónicos de un expediente electrónico.- Crees que se necesita firma electrónica? (Art. 32. 2º)