novática
Revista de la Asociación de Técnicos de Informática
MAYO - JUNIO 1999
139

SUMARIO

Novática, revista fundada en 1975, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática)

ATI es miembro de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AII y ASTIC

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica@ati.es*>
Composición, Edición y Redacción ATI Valencia
Palomino 14, 2ª, 46003 Valencia
Tlf./fax 963918531 <*secreval@ati.es*>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 <*secregen@ati.es*>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 <*secreand@ati.es*>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 <*secreara@ati.es*>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 <*gpgal@ati.es*>

Publicidad: Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica.publicidad@ati.es*>

Imprenta: Gráficas Sierra S.L., Atenas, 3, int. bajos, 08006 Barcelona.
Depósito Legal: B 15.154-1975
ISBN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix

LegisTIC

Presentación

Emilio del Peso Navarro *, Rafael Fernández Calvo **

<edelpeso@tsai.es>
<rfcalvo@ati.es>

"*La ignorancia de la Ley no exime de su cumplimiento*". Así reza un antiquísimo principio jurídico que es aplicable también a la actividad de los profesionales informáticos en los diversos ámbitos y niveles en que éstos desarrollan su labor. Y, sin embargo, la inmensa mayoría de los informáticos desconocen las normas legales que, directa o indirectamente, regulan las Tecnologías de la Información y la Comunicaciones (TIC) y que han ido surgiendo fundamentalmente durante la presente década hasta cubrir una muy amplia gama de ramas jurídicas (Derecho Civil, Penal, Mercantil, Administrativo, ...) y de materias (tratamiento de datos personales, protección del software, telecomunicaciones, propiedad intelectual, comercio electrónico ...).

El problema es que el incumplimiento de esas normas (no por mala fé sino, como indicábamos antes, por pura ignorancia) puede acarrearnos peligrosas consecuencias, que pueden ir desde cuantiosas multas a la pena de cárcel.

Para evitarlo, pero fundamentalmente para contribuir modestamente a aumentar la información y la formación de nuestros lectores sobre este aspecto habitualmente tan descuidado en la formación teórica y en la actividad práctica de los informáticos, se decidió dedicar una monografía a la legislación sobre TIC (de ahí el cabalístico acrónimo que hemos usado como título de la misma: *LegisTIC*). La monografía que ahora tienen entre sus manos es una demostración más del interés que ATI en general y nuestra revista en particular ha dedicado al tema del impacto social de la tecnología

Este interés nos ha llevado, aparte de tener desde hace años una sección específica sobre Derecho y Tecnología (hasta hace poco llamada "Derecho Privado Informático"), a ser precursores en este terreno (núm. 20 de 1978, 33 de 1980, 74 de 1988 y 96 de 1992) y, en el campo del activismo a ser ATI una de las entidades cofundadores de la CLI (Comisión de Libertades e Informática), organización que tanto ha influido en la redacción de la LORTAD y en la redacción de determinados artículos del Código Penal.

Pues bien, la monografía se abre con un artículo introductorio y panorámico de uno de los más destacados impulsores del estudio de esta disciplina en España, Miguel Angel Davara Rodríguez, promotor de los Encuentros sobre Informática y Derecho que vienen celebrándose desde hace ya trece años. A continuación se ofrecen unas reflexiones sobre la ética de los profesionales informáticos a cargo de Rafael Fernández Calvo, cuyo epílogo es el Código de Conducta Profesional de CEPIS (*Council of European Professional Informatics Societies*)

Emilio de Peso dedica los dos artículos siguientes a explicar los aspectos más destacados de la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal) y del Código Penal, mientras que Jorge Páez escribe sobre la protección de Software y la propiedad intelectual.

Internet, la red de redes, no podía faltar en esta monografía. De estudiar algunos de sus aspectos más de actualidad se encargan Javier Ribas, que reflexiona sobre el derecho a la intimidad en Internet; Isabel Hernando Collazos, que nos habla sobre la regulación del comercio electrónico en Europa, y Miguel Angel Davara Fernández de Marcos, que escribe sobre la regulación de los nombres de dominio. Tampoco podía faltar el famoso "Efecto 2000", sobre cuyos efectos jurídicos escribe Javier Cavestany.

La monografía, en la que, por razones de espacio, no hemos podido incluir algunos artículos de gran interés y que serán publicados tan pronto como sea posible, se cierra con una amplia bibliografía, que incluye tanto libros como sitios web de interés para el tema objeto de la misma.

Para finalizar esta presentación debemos señalar que hemos intentado que los artículos que componen esta monografía estuviesen escritos de manera didáctica y comprensible para personas sin formación jurídica. Esperamos haberlo conseguido pero son Vds. quienes tienen que confirmarlo. Si su respuesta es positiva y además esta monografía se convierte en un instrumento de referencia y consulta tanto Novática como estos coordinadores habremos conseguido nuestras modestas aspiraciones.

Coordinadores de la monografía

* *Emilio de Peso Navarro* es Licenciado en Derecho por la UCM y Licenciado en Informática por la UPM, así como Diplomado en Asesoría de Empresas, Derecho del Trabajo e Impuestos por la Escuela de Práctica Jurídica de la Facultad de Derecho de la UCM. Socio Director de IEE (Informáticos Europeos Expertos).

Experto en Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones, ha participado como conferenciante o ponente en numerosos Congresos nacionales e internacionales. Ha impartido conferencias y seminarios sobre la materia en las principales instituciones del país. Escribe numerosas revistas especializadas y es autor o coautor de numerosos libros, entre los que se pueden destacar "Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas" (Díaz de Santos, Madrid 1994) y "La LORTAD y la seguridad - Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal" (Díaz de Santos, de próxima publicación).

Pertenece al Ilustre Colegio de Abogados de Madrid, a la OAI/ISACA España, ALI, ATI y AUI. Es miembro de la *Information Systems Audit and Control Association*.

** *Rafael Fernández Calvo* es Licenciado en Derecho por la UCM, Graduado en Periodismo por la Escuela Oficial de Periodismo de Madrid, Diplomado en Función Gerencial por ESADE (Barcelona) e Ingeniero de Sistemas por IEC/IBM.

Ejerce como consultor independiente de Sistemas de Información y Comunicación, especialmente en temas relacionados con el uso de Internet en la empresa.

Periodista y conferenciante, es responsable de la Coordinación Editorial de la revista Novática y editor en funciones del web de ATI, ha impartido conferencias sobre el impacto social de la nuevas tecnologías y la responsabilidad legal y ética de los profesionales informáticos, y ha publicado numerosos artículos sobre estos mismos temas.

Fue representante de ATI en la CLI (Comisión de Libertades e Informática) y miembro de su Presidencia Colegiada de 1991 a 1997.

Socio de Senior de ATI y primer Presidente del Capítulo de Madrid de dicha asociación, es también miembro de la *Internet Society* y pertenece al Ilustre Colegio de Abogados de Madrid.

LegisTIC

Perspectivas del Derecho de las Tecnologías de la Información y las Comunicaciones

Miguel-Angel Davara Rodríguez
Doctor en Derecho, Director del Instituto de Informática Jurídica de la Facultad de Derecho de la Universidad P. Comillas (ICADE)

1. Una presentación del problema

La irrupción de las tecnologías de la información y las comunicaciones (**TIC**) en todos los ámbitos y actividades se produce de forma que podemos calificar de insolente; se trata del poder de la información que ya anunciaran Nora y Minc[1], y que, hoy en día, se ve no acrecentado pero sí popularmente conocido por la utilización masiva de las modernas tecnologías; el cambio producido en la estructura social implica, sin duda, una modificación de actitudes y comportamientos que el Derecho, como regulador de convivencia, debe atender.

Es así que debemos analizar la regulación jurídica de las relaciones y comportamientos que se producen con la utilización de las herramientas tecnológicas; el Derecho no puede ni debe vivir ajeno a ello; es lo que podríamos llamar el Derecho de las tecnologías de la información y las comunicaciones, que si posee alguna característica especial es debida al objeto que se pretende regular, y cuya evolución y comportamiento condicionan en gran parte la forma de pensar y de actuar del jurista, y obliga a preguntarse si nos encontramos ante un nuevo modelo de sociedad en el que se debe plantear un nuevo modelo de Derecho.

En consecuencia, el interés en regular el mundo de las **TIC's** crece llegando a límites insospechados. El impacto que el nuevo entorno de la información puede tener sobre la sociedad es tan grande que no nos permite vivir ajenos a él, sin olvidar, además, que en el mundo tecnológico, y su relación con el económico, se mueven diversos e importantes intereses que el Derecho se ve obligado a regular. Parece lógico, por tanto, que el Derecho proporcione a la tecnología una regulación jurídica que es necesaria para su desarrollo.

2. El llamado Derecho de las TIC's

Como hemos indicado, en las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las tecnologías de la información y las comunicaciones surgen los problemas acerca de cómo resolver determinados conflictos nacidos de esa relación.

Surgen también, como nuevos frutos, bienes que, al estar en el comercio de los hombres, son objeto de propiedad y, por tanto, de protección jurídica. Algunos de ellos, como los equipos o materiales que componen un ordenador, serán menos conflictivos en el momento de adscribirles a un área de protección de las ya establecidas en nuestro ordenamiento jurídico; más bien diríamos que su adscripción se produce de forma automática, por su naturaleza, en consonancia con el tipo de bien de que se trata; otros bienes, sin embargo, como los programas de ordenador, han tenido que conocer un duro camino hasta hacer efectiva su protección ante las posibles agresiones, malintencionadas o no, de aquellos que no tienen derechos sobre ellos.

De otra parte, el fenómeno tecnológico no ha traído como resultado solamente su utilización comercial y profesional, sino que con él han surgido vinculaciones y bienes hasta ahora desconocidos; de esta forma, nacen al tráfico jurídico unas relaciones consecuencia de la contratación electrónica, informática y telemática y de los nuevos productos y servicios comerciales que ven la luz con el apoyo y posibilidades de desarrollo que la tecnología les proporciona, ya que en la práctica mercantil se presenta un nuevo escenario comercial que está caracterizado por la utilización de los elementos telemáticos, de las redes abiertas y de la tecnología informática, de forma que sería imposible realizar algunos negocios si no fuera con el apoyo de las **TIC's**.

Se debe analizar también la incidencia de los medios de comunicación en el mundo empresarial, desde la óptica jurídica, asumiendo de antemano que la comunicación y el intercambio de información llevan aparejado, no solamente el enriquecimiento de la información y la posibilidad de utilizarla por más personas en diferentes lugares, sino también la difusión y acrecentamiento del error y la distorsión en la idea transmitida por el viaje efectuado entre emisor, vía de comunicación y usuario, que puede, y así ocurre de hecho en múltiples ocasiones, modificar el espíritu de lo comunicado sin variar su representación externa, con lo que las posibles comprobaciones realizadas para garantizar la fiabilidad del mensaje transmitido, y su identificación con el recibido, no siempre dan el fruto deseado al poder ser objeto de identidad solamente física.

Sin olvidar la tan aireada regulación jurídica de Internet que, con un contenido muy extenso, resulta imposible ni tan siquiera resumir por su inalcanzabilidad, pero que podemos iniciar diciendo que la puesta a disposición de un entorno seguro en Internet es necesario para aprovechar plenamente su potencial y que ese entorno seguro debe pasar, naturalmente, con la creación del marco normativo adecuado que proporcione la seguridad jurídica necesaria.

Todo ello configura el que hemos dado en denominar derecho de las **TIC's**.

3. A modo de ejemplo

Con el ánimo de enunciar algunas de las cuestiones planteadas y, naturalmente, sin finalidad limitativa, diremos, a modo de ejemplo, que nos encontramos con:

- Las llamadas **leyes de protección de datos**, que desarrollan la protección jurídica de los derechos de las personas ante la potencial agresividad de la informática, con respecto al tratamiento automatizado de sus datos de carácter personal; leyes que, en la práctica, con la publicación de la Ley Orgánica 5/1992 (**LORTAD**) y normativa que la desarrolla, están teniendo una gran incidencia en el tratamiento de la información y, en particular, en todo lo que se refiere a la defensa de la intimidad -o de la llamada privacidad- ante la potencial agresividad de las herramientas tecnológicas.

- La regulación jurídica de los derechos y obligaciones consecuentes de la creación, distribución, explotación y/o utilización del hardware y software, con su protección en los derechos de propiedad industrial o en los de propiedad intelectual, incluso con un obligado acercamiento a la protección jurídica de los productos multimedia. Atendiendo, naturalmente, de una forma especial a la protección jurídica de los programas de ordenador, considerados como un bien inmaterial, contra la llamada piratería del software.

-Los derechos y obligaciones de los creadores, distribuidores y usuarios de bases de datos, en todas las facetas contempladas en las normas y que van desde la protección a la creación de la obra hasta la denominada en un principio **protección de extracciones desleales**, que ha terminado en nuestra ley recogido como un derecho *sui géneris* cuyo 'objeto' es el de garantizar la protección a la inversión en la obtención, verificación o presentación del contenido de una base de datos.

-El amplio campo de la contratación de bienes y servicios informáticos con sus características fácticas y jurídicas, incluida la contratación informática directa por el Estado con otros países, e indirecta mediante elementos que llevan incorporados, como auxiliar a su funcionamiento, programas de ordenador.

-Las responsabilidades, derechos y obligaciones derivadas de la transferencia electrónica de fondos o de datos, incluso entre diversos países, con diferentes regulaciones jurídicas, y las responsabilidades consecuentes de operaciones en cadena, por medio de redes de comunicaciones pertenecientes a distintos territorios y bajo dispares ordenamientos jurídicos.

-La contratación electrónica, con los problemas de la validez y reconocimiento de la firma electrónica y digital, tan de moda hoy en día con la **Propuesta de Directiva europea de octubre de 1998**, y la validez probatoria de los documentos generados por medios electrónicos, informáticos o telemáticos, o que se encuentran en soportes susceptibles de tratamiento automatizado.

-El llamado **delito informático**, entendiendo por tal la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

-El denominado **tele-trabajo**, ya que las facilidades de gestión que proporciona la tecnología pueden traer un cambio en la normativa laboral; las normas de Derecho del Trabajo se referirán en el futuro más al mercado del trabajo con la variación de las costumbres sociales y su incidencia en el comportamiento humano.

-La utilización de herramientas a través de las redes de telecomunicación, ya que el correo electrónico, la posibilidad de consulta de ficheros en bases de datos y de navegar a través de redes en un mundo de servicios mutimedia, interactivos, hace nacer la explosión de nuevos servicios mediante una auténtica teoría diversificadora de la oferta, permitiendo todos los tratamientos, incluso el de imagen, en forma conjunta y ordenada, con la posibilidad de acceder unos a otros modificándose e interrelacionándose en forma dinámica y, como es lógico, surge también la necesidad de su regulación jurídica.

-El desarrollo de las telecomunicaciones y su liberalización, a partir de un mercado como el que existía, monopolista y oportunista, con una gran competencia y un futuro negocio que necesita la normativa adecuada, atendiendo, naturalmente, a la vigencia de las leyes de defensa de la competencia frente a los grandes productores y distribuidores de Informática y a los operadores de telecomunicaciones.

Y otros muchos aspectos a tener en cuenta y cuya relación aquí harían muy extenso y engorroso este trabajo.

4. Una llamada de atención a la seguridad

Los negocios actuales han creado una excesiva dependencia de las **TIC** y se han hecho particularmente vulnerables debido, en gran parte, a las características propias del tratamiento telemático; vulnerables, en principio, por la falta de seguridad física que ello conlleva; vulnerables, también, por la falta de seguridad lógica y vulnerables, por último, por la falta de seguridad jurídica.

La seguridad de los sistemas informáticos y de comunicaciones y, consecuentemente de los datos e información que en ellos se encuentren, o, si se trata de sistemas de comunicaciones, de datos e información que sobre ellos viajan, requieren técnicas, equipos y procedimientos especializados; pero hablamos de seguridad en tres aspectos: Seguridad lógica, seguridad física y seguridad jurídica. Las dos primeras, seguridad física y seguridad lógica, representan una protección *a priori*, sin embargo la seguridad jurídica podemos pensar en ella como una protección *a posteriori*,

aunque también se puede entender como *a priori* atendiendo al análisis y estudio de la prevención de los riesgos a los que puede estar expuesta una entidad por un tratamiento inadecuado de la información de acuerdo con lo contemplado en la normativa vigente.

A ello hay que añadir que la seguridad y la confidencialidad de los datos que se manejan por medio de estas tecnologías no están de otra parte asegurados, en razón, a veces, de insuficiencia de medios o de distintas calidades de transmisión de las diferentes redes, ya que existen al entrar en el mundo de las comunicaciones unas dificultades de orden técnico. El uso generalizado de la transferencia electrónica de datos tiene como consecuencia un problema de lenguaje lógico entre los diferentes equipos y redes de transmisión, de normas procedentes de las distintas formas de tratar los mensajes en la transmisión y de compatibilidad entre equipos y programas.

5. Conclusiones

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

Se abren nuevos campos de actividad; o se cierran viejos campos de actividad; o se modifican los campos de actividad; lo podemos llamar como queramos pero, lo cierto es que se cambian los hábitos y la forma de actuar en el momento de preparar, de analizar o de realizar un trabajo. Deviene con ello necesario el análisis, estudio y permanente conocimiento de la regulación jurídica de las **TIC's**.

Seguridad física, lógica y jurídica deben ser prioritarias en la implantación de los nuevos servicios, pero al mismo tiempo esa seguridad tiene que jugar un papel importante, con una dinámica de desarrollo educacional, social y económica, valiente en sus presupuestos y flexible en su realización, modificando la actuación certeramente cuando se desvíe de los fines previstos.

Para terminar, nos vamos a permitir una licencia ya que nos resulta imposible sustraernos de un pensamiento que hace tiempo nos preocupa y condiciona nuestra actividad y que no por repetitivo pierde para nosotros su fuerza, aprovechando cualquier ocasión para ponerlo de manifiesto. Por ello quisiéramos acabar diciendo que no debemos olvidar que si la eficacia y el progreso son necesarios, nunca deben ser comprados a un precio en el que esté incluido un recorte en las libertades de la persona. Por otro lado, no es conveniente separar, como día a día se va haciendo, tecnología de humanismo. Por el contrario es conveniente unir ambos términos para lograr una interrelación que justifique el progreso de la sociedad junto a su característica básica : el carácter humanitario de la persona. El desarrollo tecnológico debe ir así avanzando, en paralelo, haciendo siempre referencia al bien del género humano, en lo que podemos llamar el 'humanismo tecnológico'.

Todos debemos trabajar para colaborar en marcar bien claramente las diferencias entre lo que es, lo que puede ser y lo que debe ser, orientando el camino que debe tomar la regulación jurídica del fenómeno tecnológico en lo que damos en llamar el **Derecho de las Tecnologías de la Información y las Comunicaciones**.

6. Notas

[1] Cfr. Nora, S. y Minc, A. "La informatización de la sociedad". Informe sobre "La informatización de la Sociedad", conocido como *Informe Nora- Minc*. Traducción de Paloma García de Pruneda, F.C.E. de España, Madrid, 1983.

LegisTIC

Algunas reflexiones sobre la Etica Profesional en la Informática

Rafael Fernández Calvo
Socio Senior de ATI

<rfcalvo@ati.es>

***Resumen**: la Etica constituye un componente esencial para el correcto funcionamiento de cualquier colectividad humana. Por ello es imprescindible reflexionar sobre su importancia como marco ideal de referencia para la actividad de los profesionales informáticos. Los Códigos de Conducta profesional que elaboran las asociaciones profesionales son la plasmación de los principios que deben inspirar su actuación pero, dada la expansión continua y creciente de las TIC (Tecnologías de la Información y de las Comunicaciones) en todos los ámbitos de la vida pública y privada, dichos códigos han de situar entre sus prioridades los intereses de los usuarios finales y los de la sociedad en su conjunto..*

1. Introducción

Se dice de forma coloquial que así como el Derecho es el campo del "así debe ser", la Etica es el terreno del "ojalá fuera así". La razón es que mientras el Derecho tiene que concretarse en normas legales cuya infracción ha de castigarse por la jurisdicción competente (penal, civil, administrativa, ..), la Etica se plasma en principios más o menos generales cuya transgresión suele producir solamente un grado variable de reproche social. Esta primera diferencia entre ambos conceptos tiene su reflejo práctico de enorme transcendencia en el hecho de que mientras, en lo que se refiere al Derecho, el poder principal pertenece al Estado a través de la facultad de legislar y de juzgar (que residen en el Poder Legislativo y en el Poder Judicial, respectivamente), en lo que respecta a la Etica es cada grupo social involucrado o, en algunos casos, la sociedad en su conjunto quien tiene la iniciativa tanto para su definición (a menudo mediante Códigos de Etica o de Conducta cuando se trata de colectivos específicos) como para su puesta en práctica.

Aun así, la Etica constituye un componente esencial para el correcto funcionamiento de cualquier colectividad humana. Por ello es imprescindible reflexionar sobre su importancia como marco ideal de referencia para la actividad de los profesionales informáticos.

Pero, ¿qué es la Etica? La palabra "ética" procede del griego hJos, hábito o costumbre, y el Diccionario de la Real Academia de la Lengua Española la define como la "parte de la filosofía que trata de la moral y de las obligaciones del hombre". Esta definición, de carácter doctrinal, puede servirnos de introducción a la que nos da el autor francés J.P. Gelinier, para quien "la ética no es sino la reflexión sobre la conducción responsable de la vida en el sentido deseado", definición más empírica y orientada al comportamiento individual.

Tomando como base esta última, la *ética profesional* podría definirse como "la aplicación al ejercicio de la propia actividad laboral de criterios personales y colectivos de responsabilidad individual y social", definición que es la que emplearemos en este artículo al referirnos al campo del ejercicio profesional de las TIC (Tecnologías de la Información y de las Comunicaciones) en cualquier ámbito: el de la docencia, el de la investigación o de la práctica como técnico o consultor, dependiente o independiente, etc.

Pero, en el campo de la Ciencia y la Tecnología en general, y en el de las TIC, en particular, ¿se puede hablar de una ética profesional abstracta, desligada de su impacto social?; más aun, ¿es suficiente hoy día una ética solamente para profesionales?

El divorcio entre Tecnología y Humanidades

Uno de los principales problemas que se plantean respecto a las relaciones del profesional informático con el Derecho y con la Etica es el desconocimiento casi absoluto que aquél suele tener respecto a los aspectos de dichas disciplinas que afectan a su trabajo, desconocimiento que el autor de este artículo ha comprobado en repetidas ocasiones en los últimos quince años, tanto en su labor como ponente de numerosos congresos, jornadas, charlas, conferencias y mesas redondas organizadas por la **CLI (Comisión de Libertades e Informática)**, por ATI o por otras entidades en diferentes lugares del país, como en su trabajo como consultor.

Este desconocimiento tiene su origen fundamental en que, hasta hace muy pocos años, al menos en España, casi ningún Plan de Estudios informáticos universitarios, de grado medio o superior (por no hablar, claro está, de centros no universitarios), incluía dichas disciplinas. Hoy sí las incluyen, al menos el llamado Derecho Informático, pero en no pocos casos, desgraciadamente, como asignaturas de las llamadas "Marías".

Yendo más a la raíz, esa situación responde a la idea de que la Ciencia y la Tecnología nada tienen que ver con las Humanidades, entendidas en su sentido más amplio; idea

funesta y obsoleta, hija decimonónica del positivismo científico y de la arrogancia filosófica, que llevaba, y aún lleva, a que los planes de estudios universitarios de cada una de esas ramas del saber ignorasen a la otra.

Si nos concentramos en la Informática, hay que partir de la premisa de que un profesional informático de nuestro tiempo no puede ni debe limitarse a conocer el "cómo" (es decir, los aspectos tecnológicos) de la disciplina que practica sino también los "por qué" y los "para qué", elementos clave de cualquier visión ética del ejercicio profesional. El conocimiento de los "por qué" y los "para qué" se hace totalmente imprescindible para los informáticos porque las TIC, un sector en el que avanza a velocidad de vértigo y en el que se mueven tantos y tan importantes intereses, tienen un impacto cada vez mayor sobre todas las esferas, públicas y privadas, de la actividad humana.

El problema de fondo es que, si nos concentramos solamente en el "cómo", en nuestras sociedades desarrolladas se producirá de forma paulatina e irreversible un desequilibrio entre el superdesarrollo tecnológico y el subdesarrollo sociocultural. Siguiendo al escritor José Luis Sampedro, habría que proclamar que "modernizar las ideas es tan importante como modernizar las tecnologías", pues los ciudadanos en general, y los profesionales informáticos en particular, hemos de ser conscientes de que estas nuevas tecnologías son herramientas de gran importancia que pueden ayudar a que la sociedad se oriente en una o en otra dirección: la Sociedad de la Información y del Conocimiento, en la que el centro de gravedad sería la persona y la sociedad misma, o la Sociedad Informatizada, en la que tendrían la primacía las herramientas tecnológicas y los intereses de quienes las producen.

Por todo ello se hace necesario y urgente que los profesionales informáticos vayamos siendo progresivamente educados en temas tales como una ética profesional que tenga en cuenta el entorno social de las TIC y sus efectos sobre la sociedad y los individuos, lo que el profesor Fernando Sáez Vacas ha denominado "Socio-tecnología", una rama del saber que contempla a las TIC en su contexto social.

Con el razonamiento anterior creemos haber respondido de forma negativa a la primera pregunta que nos planteábamos (¿se puede hablar de ética profesional en abstracto?) y pasaremos a intentar dar una respuesta a la segunda: ¿es suficiente una ética profesional solamente para profesionales?

El nuevo panorama "usuariocéntrico"

Es un hecho evidente que hace apenas 25 años la inmensa mayoría de quienes utilizábamos las TIC éramos los profesionales informáticos que las manejábamos en las diversas fases de su ciclo de vida (investigación, desarrollo, implantación, formación, operación, asistencia técnica, ...). Hoy, por el contrario, el número de usuarios de las TIC (usuarios finales, es decir, personas que no son profesionales informáticos) ha crecido de forma espectacular durante la última década, superando al número de dichos profesionales en órdenes de magnitud, y continuará creciendo a un ritmo incluso superior durante los próximos años pues así lo auguran la difusión de la informática personal en todos los ámbitos de la vida social y económica, la convergencia entre la Informática y las Telecomunicaciones, y la expansión de Internet.

Junto a la evidencia del crecimiento de la cantidad de usuarios se produce una interesante característica cualitativa inherente al uso de las TIC: su carácter activo, pues a diferencia de los usuarios de otras tecnologías de gran difusión, los usuarios de las TIC, para conseguir cualquier resultado, tienen que interactuar de forma activa con sus herramientas sin que sea posible ante ellas una actitud pasiva. Un ejemplo de esto es la enorme diferencia de actitud existente entre quien ve la televisión y quien "navega" por la red.

A la vez hay que señalar que estas herramientas (programas y procesadores esencialmente) que requieren una actitud activa de quien las usa tienen un origen oligopólico pues son producidas por un puñado de grandes marcas multinacionales. Estas pueden imponer los ritmos de obsolescencia de sus productos (y de la consiguiente y casi inevitable renovación de los mismos en plazos cada vez más cortos) en función de sus intereses de negocio, muy respetables sin duda alguna pero que no pueden ser el único valor relevante en una sociedad democrática. El resultado final es que a la vez que las herramientas tecnológicas requieren una actitud activa, los centenares de millones de usuarios finales de las TIC en todo el mundo tienen muy poca autonomía y escasas posibilidades de opciones alternativas respecto a las mismas.

Una conclusión parece evidente: los protagonistas de las TIC, desde hace ya algunos años, no son sólo los informáticos sino que lo son cada vez más (1) las amplias capas de la población que las utilizan diaria y directamente en sus centros de trabajo o de estudio y en sus propios hogares; (2) el conjunto de la sociedad, incluyendo también a aquellos que no usan las TIC directamente pero lo hacen indirectamente a través de los múltiples servicios y productos que sí las incorporan.

Dado que es previsible que la mezcla de estos fenómenos cuantitativos y cualitativos tendrá cada día más influencia en el modo en que los informáticos enfocamos la práctica profesional de su actividad desde una perspectiva ética, la respuesta a nuestra segunda pregunta (¿es suficiente una ética profesional solamente para profesionales?) tiene también que ser negativa por fuerza.

La conclusión es que en el sector de las TIC es necesaria una ética profesional informática que vaya más allá de los intereses corporativos de los informáticos y sitúe entre sus prioridades la cooperación con aquellas organizaciones de la sociedad civil y de las Administraciones Públicas que defienden los intereses individuales y colectivos en diversos ámbitos. Hablamos, por ejemplo, de asociaciones de consumidores, de grupos de defensa de los derechos humanos o de

organizaciones de ayuda a los países en vías de desarrollo y también de instituciones públicas nacionales e internacionales (en nuestro país pensemos en el Defensor del Pueblo y en la Agencia de Protección de Datos, y en las instituciones equivalentes de las diversas Comunidades Autónomas).

En primera fila de quienes promuevan este nuevo impulso ético deben estar, sin duda alguna, las asociaciones que agrupan a los profesionales informáticos: una de sus principales herramientas son sin duda los Códigos de Conducta Profesional (también llamados Códigos de Etica Profesional).

Códigos de conducta profesional en el ámbito informático

En 1968, en Estados Unidos, *ACM (Association for Computing Machinery)*, la mayor y más antigua de las asociaciones profesionales informáticas de todo el mundo, elabora el primer código de conducta profesional en el campo de la informática. En 1970 aparece el aprobado por la *BCS (British Computer Society)*, al que siguen otros en años sucesivos (ver "Material de consulta" en esta misma monografía). En España, en 1974, hubo un proyecto elaborado por CITEMA, no constándonos que ninguna de las asociaciones profesionales informáticas españolas haya tomado iniciativa alguna, al menos públicamente, en esta dirección desde entonces.

Pero permítasenos otra pregunta: ¿cuál es la utilidad de los códigos de conducta? En una interesante y documentada ponencia presentada al III Congreso Internacional sobre Etica y Computadores (ETHICOMP 96) y que lleva por título "Profesionalidad y responsabilidad ética en la Informática", el profesor Porfirio Barroso explica que, en primer lugar, dichos códigos "sirven de guía de acción no solamente para los profesionales, profesores y estudiantes de informática sino también para quienes, no perteneciendo a este sector, emplean esas tecnologías; en segundo lugar, aumentan la comprensión por los no especialistas y por el público de las nuevas cuestiones éticas que emergen en la Sociedad de la Información, ejerciendo así una función educativa; finalmente, facilitan que, tras un cierto periodo de prueba, las más importantes de esas nuevas cuestiones pasen a ser reguladas legalmente de forma adecuada".

En esa misma ponencia, el profesor Barroso describe los resultados de un exhaustivo trabajo de análisis de cincuenta códigos de ética informática en vigor en numerosos colegios, asociaciones profesionales y empresas del sector de la informática de todo el mundo. El citado profesor y veinte de sus alumnos realizaron un análisis lexicográfico de esos cincuenta códigos de ética, durante el cual identificaron cuarenta y siete principios o conceptos deontológicos.

Los quince principios más comunes en dichos códigos, de mayor a menor, son los siguientes:
1. Responsabilidad profesional
2. Cumplimiento del código
3. Secreto profesional
4. Demostrar competencia
5. Integridad profesional
6. Verdad, objetividad
7. Primacía del bien común
8. Preparación académica
9. Empleo de medios justos y honestos
10. Colaboración en el desarrollo de la Informática
11. Dignidad, honestidad
12. Lealtad a la empresa y al público
13. Respeto a las leyes
14. Solidaridad profesional
15. Obligaciones con el público

ATI y los códigos de conducta

A lo largo de su ya larga historia (32 años) ATI, entidad editora de Novática, ha mostrado una preocupación innegable por el impacto social de la Informática; recordemos a este respecto la creación de la ya citada CLI y las diversas monografías publicadas por esta misma revista. Sin embargo, nunca llegaron a cuajar los diversos intentos de elaborar un código de conducta profesional propio, aunque los Estatutos vigentes, aprobados en 1992, en su artículo 2.1.4 dicen literalmente que un socio de ATI puede perder su condición de tal cuando "viole los Códigos de Conducta profesional adoptados por ésta (la asociación)".

No obstante, la pertenencia de ATI a CEPIS (*Council of European Professional Informatics Societies*), primero a través de FESI desde 1992 y de forma autónoma desde 1997, ha llevado a la adopción automática como propio del Código de Conducta elaborado por dicha organización. Dicho código, cuya traducción al castellano aparece en esta misma monografía, está constituido por una serie de principios básicos que las sociedades miembro de CEPIS se comprometen a emplear como base para elaborar sus propios códigos.

Ahora bien, dijimos anteriormente que el usuario ha pasado a ser el protagonista esencial de las TIC y en este nuevo campo ATI sí está teniendo el protagonismo que le corresponde por ser la asociación más antigua y más numerosa de las que agrupan a los profesionales informáticos en nuestro país. Nos referimos a dos experiencias pioneras en este terreno: la primera es el proyecto *ECDL (European Computer Driver Licence)*, promovido por CEPIS y la segunda el Código de Conducta de Usuarios de ATInet, la red asociativa de la asociación. Las describiremos muy brevemente.

ECDL (*European Computer Driving Licence*)

El proyecto **ECDL** (que en castellano podríamos traducir como "Certificado de Capacitación para el Uso de Ordenadores") surgió originariamente en Finlandia a principios de esta década, siendo actualmente uno de los proyectos piloto de la Unión Europea para la implantación de la Sociedad de la Información.

Los objetivos principales de la ECDL son preparar a los ciudadanos europeos para la Sociedad de la Información y elevar el nivel de cultura, capacitación y formación informática de los trabajadores europeos en el área de las Tecno-

logías de la Información y de las Comunicaciones. Hay que subrayar que en el primero de sus módulos incluye un apartado dedicado a la conducta de los usuarios e incluye temas tales como privacidad y los derechos y deberes de los usuarios, considerados como elementos esenciales para su formación. Para más información visitar *http://www.ecdl.com*

Código de Conducta para Usuarios de ATInet

Este tipo de códigos es todavía bastante infrecuente y por eso es interesante señalar que uno de ellos ha surgido en nuestro país. Lo elaboró y aprobó ATI en Enero de 1997 con objeto de regular su propia red asociativa, llamada ATInet. El código se basa en cuatro principios esenciales: la autorregulación de los usuarios, el derecho constitucional a la libertad de expresión, el respeto a los derechos ajenos y la atención a la ecología de la red, entendida como un uso adecuado de los recursos tecnológicos disponibles.

Tiene dos particularidades: por una parte, los usuarios de ATInet deben comprometerse a cumplir estas regla antes de ser dados de alta; por otra, el usuario puede ser dado baja de la red (e incluso de la misma asociación) en caso de infracciones graves del código..

Al tratarse de un servicio limitado a miembros de una determinada organización, sus normas no son trasladables a la red de forma automática pero conocerlas puede resultar de utilidad para mostrar la visión de una asociación profesional de informáticos sobre cuál *debería ser* la conducta de los usuarios de la red, unos usuarios especialmente cualificados por su condición de informáticos. Dado que, aunque están disponibles íntegramente en el servidor web de ATI, en *http://www.ati.es/socios/introATInet.html*, lo están por el momento solamente para socios de ATI, reproducimos su introducción: "Partiendo de la conveniencia de que la autorregulación de los propios usuarios predomine, siempre que ello sea posible, sobre cualquier control externo y del reconocimiento tanto del derecho constitucional a la libertad de expresión como de la necesidad de que se haga un uso responsable de la misma, el buen funcionamiento del servicio ATInet requiere la sumisión a unos principios éticos y a unas reglas de uso elementales, principios y reglas que el solicitante se compromete a cumplir desde el momento en el que se produzca su alta en el servicio y que se recogen en las siguientes Normas de Conducta ...".

En las condiciones de alta en ATInet aparecen otros aspectos relevantes relacionados con la conducta profesional. Nos referimos a la responsabilidad del usuario respecto a la utilización legal del software, a la difusión de virus y similares, y a la aplicación de las normas legales en cuanto a la protección de los datos personales.

Conclusiones

1. Las **TIC (Tecnologías de la Información y las Telecomunicaciones)** tienen una difusión creciente y un impacto social, económico y cultural de gran relevancia, lo cual constituye un hecho de enorme relevancia para la definición y aplicación de la ética profesional en el campo de Informática.
2. Hoy el protagonista de las TIC no es tanto el profesional informático como el usuario final. Por ello la regulación de la conducta profesional informática también debe tener muy en cuenta los intereses y necesidades de éste último.
3. Las TIC ofrecen una gama muy amplia de oportunidades y amenazas para el presente y el futuro de la llamada "Sociedad de la Información". El profesional informático debe conocerlas y valorarlas desde un enfoque que, además de tecnológico, ha de ser también social.
4. Los códigos de conducta profesional son una importante herramienta no sólo para la regulación de la actividad de los informáticos sino que aportan a la sociedad una valoración cualificada sobre las TIC, facilitando que, tras un cierto periodo de prueba, las más importantes de las nuevas cuestiones pasen a ser asumidas por la sociedad y reguladas legalmente de forma adecuada.

LegisTIC

Código de Conducta Profesional de CEPIS*

* CEPIS (*Council of European Professional Informatics Societies*) fue creado en 1988 y agrupa a 29 asociaciones de 24 países europeos que representan a 150.000 profesionales informáticos. ATI es representante español en dicho organismo, por lo cual de hecho este Código de Conducta se aplica automáticamente a nuestra Asociación.

Traducción: Rafael Fernández Calvo

1. Introducción

Este código establece los principios generales de conducta profesional y ética que deben incluirse en los Códigos de Conducta que adopten las sociedades miembro de **CEPIS**.

Sus principios reconocen que las actividades de carácter profesional imponen cuatro deberes específicos a quienes las practican, que son estar al servicio de: el interés público, el empleador y el cliente, la profesión informática y el profesional informático.

Los anteriores deberes implican una serie de obligaciones que han de cumplir los profesionales informáticos, tal como se detalla a continuación.

2. Protección del interés público y cumplimiento de las leyes

· Salvaguardar la salud pública, la seguridad y el medio ambiente.
· Reconocer los derechos de terceros.
· Evitar causar daños a los derechos de propiedad intelectual.
· Reconocer los derechos individuales y colectivos a la privacidad de la información.
· Conocer y comprender la legislación, normativas y estándares aplicables, y hacer que los profesionales informáticos las cumplan en su trabajo.
· Reconocer los derechos humanos básicos y evitar aquellas acciones que tengan un efecto adverso sobre dichos derechos.

3. Responsabilidad hacia empleadores y clientes

· Cumplir las obligaciones de su trabajo profesional de forma que se satisfagan los requerimientos del empleador y del cliente, concienciando a estos de las consecuencias negativas que pueden derivarse de ignorar o desautorizar su opinión profesional.
· Cumplir las obligaciones de su trabajo profesional de acuerdo con los objetivos de plazo y presupuesto, debiendo notificar tan pronto como sea posible al empleador o al cliente sobre la imposibilidad de cumplir dichos objetivos.
· No ofrecer ni proporcionar a terceros incentivo alguno a cambio de que proporcionen clientes, a menos que los clientes sean informados fehacientemente de este particular.
· No difundir, o no autorizar la difusión de, información confidencial conseguida con motivo de su actividad profesional excepto en el caso de tener autorización previa y por escrito del empleador o del cliente, ni utilizar dicha información para el beneficio personal o de terceros.

4. Dignidad profesional y promoción de la profesión

· Proteger la reputación de la profesión informática y la mejora de sus estándares profesionales mediante la participación personal en su desarrollo, uso y regulación, así como evitar realizar acciones que afecten negativamente el buen nombre de la profesión.
· Avanzar en el conocimiento y el aprecio públicos de la Informática y contrarrestar informaciones falsas o tendenciosas que puedan perjudicar a la profesión.
· Promocionar el desarrollo profesional de, y dar apoyo a, los colegas de profesión así como abrir camino a quienes se incorporen a la misma.
· Actuar con integridad hacia los colegas de profesión y hacia los miembros de otras profesiones con los que se colabore laboralmente y evitar cualquier actividad incompatible con el *status* profesional.

5. Competencia, ética e imparcialidad

· Mejorar los conocimientos profesionales personales y estar al día de los avances técnicos relevantes en cada caso, así como evitar fingir niveles de competencia que no se poseen.
· Aceptar la responsabilidad profesional por el trabajo realizado, incluyendo el trabajo realizado bajo su dirección por subordinados y asociados, y no interrumpir un encargo profesional sin razones justificadas y sin dar un preaviso razonable.
· Evitar aquellas situaciones que puedan dar lugar a un conflicto de intereses con otros profesionales o con clientes, así como informar previamente y con detalle a los clientes de la posibilidad de que se produzca dicho conflicto.

LegisTIC

La protección de los datos de carácter personal

Emilio del Peso Navarro
Abogado y Ldo. en Informática, socio Director IEE (Informáticos Europeos Expertos), socio de ATI

<edelpeso@iee.es>

Resumen: *los avances tecnológicos han propiciado la creación de grandes almacenamientos de datos, lo que facilita la obtención de perfiles de las personas que atentan a su derecho a la intimidad. El Derecho debe proteger esa intimidad y a ello se dedican las leyes de protección de datos existente en nuestro continente desde hace algunas décadas. La seguridad de esos datos es algo primordial, sin embargo en nuestro país, seis años después de la promulgación de la* ***LORTAD*** *aún se encuentra pendiente de desarrollo su Reglamento de Seguridad. Consideramos que la aprobación de este Reglamento puede tener gran influencia para que por fin se apruebe en España esa asignatura pendiente que es la cultura de la seguridad.*

1. Introducción

Hace unos pocos meses se cumplieron los cincuenta años desde la publicación de la obra de George Orwell, *1984* en la que tenía gran protagonismo el siniestro "Gran Hermano" (*Big Brother*), que con su gran ojo electrónico se adentraba en nuestra intimidad quedando al descubierto nuestros pensamientos más íntimos.

Pasado medio siglo, miles de pequeños *big brothers* tratan de recopilar información sobre nuestras personas haciendo cada vez más grandes y valiosos esos almacenamientos masivos de información (*data warehouses*), de los que se pueden extraer perfiles cuasi perfectos de las personas.

La información siempre ha sido valiosa; ya en el pasado el emperador Sun Tsi hablaba de la importancia que tanto para el general como para el emperador tenía el conocimiento previo.

En la época actual su valor ha crecido exponencialmente; así vemos como gurús de la anticipación como Peter F. Drucker desde el mundo de la gestión nos habla de la Sociedad del Saber; Herbert A. Simon, desde el mundo de la Inteligencia Artificial, de la Sociedad del Conocimiento, y Pérez Luño, desde el mundo del Derecho, de la Sociedad de la Información.

En realidad lo que ha sucedido es que los avances tecnológicos han eliminado prácticamente los factores: tiempo y espacio. Así las informaciones que antes eran parciales y se encontraban dispersas ahora se pueden tratar en masa y de forma organizada. El aumento de valor ha sido considerable.

La aparición de redes tipo Internet ha colaborado a una más rápida y mayor difusión de la información a través del planeta.

Por otro lado los datos nominativos, que antes tenían un valor relativo, debido a la dinámica de los negocios y a la globalización de la economía han experimentado un aumento exponencial de valor.

Hoy día en el mercado negro de la información se cotiza la vida laboral de una persona, su registro en la Seguridad social y, como se ha visto en los medios de comunicación, hasta sus datos como parado. Su información tributaria, su solvencia patrimonial o su actitud a la hora de hacer frente al cumplimiento de sus obligaciones dinerarias, así como sus gustos o aficiones, son datos que las empresas dedicadas a este comercio buscan con avidez para cruzar los diferentes ficheros y así obtener otros con enorme valor añadido que poner a la venta en el mercado.

Cada vez es más importante realizar una publicidad dirigida y para ello las empresas dedicadas a estos menesteres necesitan conocer más información sobre nuestras personas lo que a la postre se traduce, gran número de veces, en un atentado a nuestra intimidad.

2. Intimidad y privacidad

La intimidad de los seres humanos siempre ha estado en el punto de mira de los opresores; numerosos ejemplos hemos tenido a lo largo del siglo que termina.

La desaparición prácticamente de la intimidad es lo que se persigue en las tres obras de ficción de la antiutopía: *Nosotros*, de Yevgueni Zamiatin, con su mundo de cristal en el que casi siempre se está a la vista de todos; *Un mundo feliz*, de Aldous Huxley, con las actuaciones en comunidad en la que ésta prima siempre sobre el individuo, y la ya citada *1984*, de George Orwell.

Los legisladores españoles fueron conscientes de la importancia que tenía salvaguardar la intimidad de las personas y su defensa la incluyeron en uno de los Títulos más importantes de la Constitución: el Primero, referido a los derechos y deberes fundamentales de las personas.

Así el artículo 18, que consta de cuatro puntos, se refiere específicamente al derecho a la intimidad y a la inviolabilidad del domicilio. El artículo se refiere a la intimidad literalmente en dos puntos: el primero y el cuarto.

En el punto 1 se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen y fue desarrollado en la Ley Orgánica 1/1982 de 5 de mayo, completada con la Ley Orgánica 3/1985, de 29 de mayo.

El artículo 18.4 garantiza el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos desde otro plano, frente a los avances tecnológicos que se están produciendo.

Entendemos que el legislador aquí fue algo duro al tratar de limitar el uso de la Informática para garantizar dichos

derechos (quizás hubiese sido mejor decir cuidar del buen uso de la Informática).

El primer problema que se nos presenta al tratar de fijar los límites del derecho de las personas a su intimidad es lograr una definición adecuada de ésta. El concepto de intimidad está todavía lejos de haber sido acuñado con claridad puesto que es muy evolutivo al hallarse condicionado por el contexto histórico, social, cultural y tecnológico.

Luis García San Miguel nos propone la siguiente definición: "Posibilidad de que algo de lo que hacemos o lo que somos (sean cuáles sean los confines de ese algo) no sea conocido por los demás y, si fuere conocido por algunos, éstos no lo den a conocer a otros".

En el pasado, la defensa de nuestros datos, en definitiva de nuestra intimidad, era relativamente fácil pues prácticamente bastaba con no comunicárselos a nadie, pero con los avances de la sociedad cada vez son más los datos que, sin que seamos nosotros quiénes los comuniquemos, van ingresando en diferentes ficheros y bases de datos.

Se establece una especie de circulo concéntrico exterior al de la intimidad que igualmente nos rodea.

A esa parcela exterior a nuestra intimidad, pero coligada a ella, y en cierto modo como extensión de la misma, se la viene denominando "privacidad".

Para Davara Rodríguez, es un término "al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona -su titular- y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad".

Por otra parte, la posibilidad de que los demás puedan tener datos nuestros aunque nosotros no se los hayamos proporcionado nos debe permitir conocer quién tiene esos datos, de dónde los ha conseguido y para qué los quiere, lo que en definitiva viene a significar el derecho a la autodeterminación informativa.

3. Normativa legal

La protección de los datos de carácter personal en España lo regula la **Ley Orgánica 5/1992** de 29 de octubre, de **Regulación del Tratamiento Automatizado de los datos de carácter personal** (**LORTAD**) y normas complementarias.

En un primer análisis de la Ley nos encontramos con tres aspectos muy importantes y en cierto modo negativos.

a) Se trata de una Ley Orgánica pero gran parte de ella, en virtud de su Disposición Final Tercera, tiene el **carácter de ordinaria.** Esto se justifica, en parte, por la continua evolución de las tecnologías y la necesidad de adaptar la Ley a estos cambios, sin tener las consecuencias de tramitación y jerarquía que ello conllevaría si toda la Ley tuviese carácter orgánico.

b) **Abuso de las excepciones:** si comenzamos a estudiar gran número de artículos, en principio nos satisfacen por entender que defienden cumplidamente nuestros derechos. Esto ocurre sólo hasta la mitad del artículo pues ahí aparece la palabra "excepto" y a partir de ahí se enfría bastante nuestro entusiasmo.

c) **Contínua remisión a la vía reglamentaria:** se abusa de la remisión a una posterior reglamentación del contenido de los artículos. Entendemos que en algunos casos hay que hacerlo pues una ley de este tipo no debe tener un carácter casuístico, pero siempre existe un término medio entre una ley excesivamente casuística y una ley desarrollada en gran parte por vía reglamentaria.

Como ejemplo puede valer el desarrollo reglamentario del artículo 9 de la LORTAD, que trata de un tema tan importante como el de la seguridad y que casi siete años después de la promulgación de la Ley sigue sin ser aprobado. La Ley se basa en los siguientes principios:

Principio de finalidad: antes de la creación de un fichero de datos de carácter personal ha de conocerse el fin del mismo. Este principio, a su vez, engloba otros dos: el principio de pertinencia y el de utilización abusiva.
Principio de pertinencia: los datos deben ser pertinentes, es decir, estar relacionados con el fin perseguido al crearse el fichero.
Principio de utilización abusiva: los datos recogidos no deben ser utilizados para otro fin distinto a aquél para el que fueron recabados.
Principio de exactitud: el responsable del fichero debe poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día.
Principio de derecho al olvido: los datos deberán desaparecer del fichero una vez se haya cumplido el fin para el que fueron recabados.
Principio del consentimiento: el tratamiento automatizado de los datos requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa contemplándose algunas excepciones y teniendo el carácter de revocable.
Principio de los datos especialmente protegidos: se debe garantizar de forma especial el tratamiento automatizado de los datos de carácter personal cuando ellos se refieran a ideología, religión o creencias del afectado, así como los referentes a su origen racial, salud, vida sexual o a la comisión de infracciones penales o administrativas.
Principio de seguridad: el responsable deberá adoptar las medidas necesarias de índole física, organizativa o lógica con objeto de poder garantizar la seguridad de los datos de los ficheros.
Principio de acceso individual: cualquier persona tendrá derecho a saber si sus datos son tratados de forma automatizada y a tener una copia de los mismos. En el caso de que estos sean inexactos o se hubiesen conseguido de forma ilegal tiene derecho a que sean corregidos o destruidos.
Principio de publicidad: es preciso que exista un fichero público en el que figuren los diseños de los ficheros de datos de carácter personal, tanto los de titularidad pública como privada.

De estos principios se derivan los siguientes derechos: impugnación, información, acceso, rectificación, cancelación y tutela.

Las sanciones que se fijan por incumplimiento son elevadas llegando en el caso de los ficheros privados hasta cien millones de pesetas y en casos extremos a la inmovilización de los ficheros.

Por **Real Decreto 428/1993** de 26 de marzo se aprobó el **Estatuto de la Agencia de Protección de Datos**. Ésta es un

órgano independiente garante de la defensa de los derechos de los afectados respecto a sus datos de carácter personal.

La Agencia de Protección de Datos se estructura en los siguientes órganos: Director de la Agencia de Protección de Datos, Consejo Consultivo, Registro General de Protección de Datos, Inspección de Datos, Asesoría Jurídica y Secretaría General. El Director será designado por el Gobierno a propuesta del Ministro de Justicia de entre los miembros del Consejo Consultivo. Su mandato durará cuatro años y sólo cesará por las causas previstas en el artículo 35. El Director de la Agencia de Protección de Datos gozará de plena independencia y ejercerá su cargo con dedicación absoluta y total objetividad, no estando sujeto a mandato imperativo alguno, ni recibirá instrucciones de ninguna autoridad. Las potestades de la Agencia de Protección de Datos son las siguientes: reguladora, instructora, inspectora, sancionadora e inmovilizadora.

Por **Real Decreto 1332/1994**, de 20 de junio, se desarrollaron determinados aspectos de la LORTAD entre los que se encuentran los procedimientos a seguir para ejercitar los derechos. Estos son los siguientes: acceso, reclamación, recurso, indemnización y sancionador.

La Agencia de Protección de Datos desde su creación ha publicado cinco Instrucciones:
Instrucción 1/1995, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito.
Instrucción 2/1995, de 4 de mayo, relativa a las medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
Instrucción 1/1996, de 1 de marzo, relativa a los ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
Instrucción 2/1996, de 1 de marzo, relativa a los ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

4. Situación actual

En el momento presente nos encontramos respecto a la protección de los datos de carácter personal en una encrucijada en la que se dan las siguientes circunstancias:

Recursos de inconstitucionalidad de la LORTAD. Se encuentran pendientes de resolución los recursos presentados por el Grupo Popular, el Defensor del Pueblo, el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento catalán contra varios de los artículos de la Ley. Han pasado ya más de seis años desde el planteamiento de los recursos.

Reglamento de Seguridad que desarrolla el artículo 9 de la Ley. Existe un Proyecto de Reglamento que prácticamente ya ha superado todos los trámites previos pendiente de aprobación. Han transcurrido ya casi siete años desde la promulgación de la Ley.

Transposición de la Directiva Comunitaria 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y la libre circulación de éstos. El plazo para efectuar la transposición a nuestro ordenamiento jurídico terminó el 23 de octubre del pasado año. En estos momentos existe un Proyecto de Ley Orgánica que fue publicado en el Boletín Oficial de las Cortes de 31 de agosto pasado. Han transcurrido cuatro años desde la publicación de la Directiva y aún está pendiente la transposición.

Vemos pues que la situación es interesante y los motivos por los que hemos llegado a esta situación muy criticables pero entendemos que un artículo para una revista no es el lugar apropiado para ello.

5. Conclusiones

Desde la experiencia conseguida en los seis años transcurridos desde la promulgación de la LORTAD podemos llegar a las siguientes conclusiones:
- a pesar de sus muchos defectos, de sus enormes lagunas y de los errores cometidos en su aplicación consideramos que su existencia ha sido positiva habiéndose avanzado en estos años en el respeto hacia el derecho a la intimidad de las personas.
- ha sido una pena no haber aprovechado los tres años que permitía la Directiva para su transposición al Derecho español para realizar una verdadera reforma de la LORTAD y no una simple y ligera adaptación.
- es imperdonable que a estas alturas no haya sido aprobado el Reglamento de Seguridad que podía llevar rodando seis años, con sus defectos si se quiere, pero con la enorme virtud de poder terminar con esa asignatura pendiente de nuestro país: la **falta de una cultura de la seguridad.**
- la experiencia nos ha demostrado la necesidad de utilizar una metodología cuando se trata de implantar la aplicación de la LORTAD en una organización y lo importante que muchas veces es contar con personas ajenas a aquélla.
- la lectura de la Ley tiene dos visiones. Una de ellas nos puede parecer negativa pues nos supone obligaciones, gastos y problemas que nos proporciona su aplicación, y otra que tiene que ser enormemente positiva pues significa la defensa de nuestro derecho a la intimidad.
- aún existe un gran desconocimiento de la Ley como hemos podido observar en nuestros seminarios por diferentes provincias de España, tanto peninsulares como insulares.
- como siempre decimos, entendemos que es más fácil criticar que crear pero en cualquier caso en nuestras críticas lo que tratamos es de poner un granito de arena en el logro de una buena Ley.

6. Bibliografía

Herranz Ortiz, Ana Isabel; *La violación de la intimidad en la protección de datos personales.* Dykinson. Madrid. 1998.
Davara Rodríguez, Miguel Ángel; *Manual de Derecho Informático. Aranzadi.* Pamplona. 1997
La protección de datos en Europa: principios, derechos y procedimientos. Grupo Asnef/Equifax y Universidad Pontificia Comillas. ICAI/ICADE. Madrid 1998.
Heredero Higueras, Manuel; *La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal.* Tecnos. Madrid. 1996.
Murillo de la Cueva, Pablo Lucas; *El derecho a la autodeterminación informativa.* Tecnos. Madrid. 1990.
Peso Navarro, Emilio del y Ramos González, Miguel Ángel; *La LORTAD: análisis de la Ley.* Díaz de Santos. Madrid. 1998.

LegisTIC

Emilio del Peso Navarro
Socio de IEE (Informáticos Europeos Expertos)

Las Tecnologías de la Información y las Comunicaciones en el Código Penal

Resumen: *los juristas debemos realizar un esfuerzo para superar la tendencia congénita a escanciar el vino nuevo de las cuestiones que emergen del cambio social y tecnológico en los odres viejos conceptuales y metódicos de la dogmática jurídica tradicional* (*"Manual de Informática y Derecho".* Pérez Luño).

1. Introducción

El desarrollo de las nuevas tecnologías de la información y su implantación cada vez más creciente en nuestra sociedad han hecho posibles nuevas modalidades de ataques a bienes jurídicos importantes, algo impensable en un pasado aún cercano. Estas nuevas tecnologías, bien aplicadas, sirven para lograr un mayor bienestar, para eliminar trabajos rutinarios y molestos inclusive para exaltar los valores de la persona; pero en manos criminales pueden resultar una potente arma para atacar la organización social.

La **Ley Orgánica 10/1995**, de 23 de noviembre, que aprobó el Código Penal, trata de hacer frente a estas nuevas situaciones en una sociedad que algunos sociólogos como David Lyon han venido en denominar Sociedad de la Vigilancia, economistas como Peter Drucker, Sociedad del Saber, y juristas como Pérez Luño Sociedad de la Información. En realidad, aunque las denominaciones parezcan divergentes, quizás debido al origen de cada especialista (la Sociología, la Economía y el Derecho), hay una especie de unicidad en las mismas pues lo que está detrás de todo ello es la posibilidad, cada día mayor, de almacenar información, de recuperarla rápidamente y de enviarla asimismo de forma casi instantánea al lugar que elijamos de la Tierra y no sólo eso: lo que se envía cada vez tiene un mayor componente de conocimiento, lo que en definitiva viene a representar poder.

El gran poder generado por esas posibilidades hace que el mundo que nos rodea cambie velozmente, lo que tiene efectos muy positivos; ahora bien, esa nueva fuerza también puede caer en manos criminales. Para evitarlo y, si esto no es posible, para punirlo, es necesario tomar las precauciones adecuadas.

Esos bienes jurídicos a que antes aludíamos debemos protegerlos y una forma de hacerlo es adoptando las necesarias medidas de seguridad, uno de cuyos aspectos, como sabemos, es el jurídico, que es el que trata de afrontar, entre otros cuerpos legales, el Código Penal.

Este tiene gran importancia en el ordenamiento jurídico de una sociedad civilizada. Como se dice en la Exposición de Motivos de la Ley, el Código Penal define los delitos y faltas que constituyen los presupuestos de la aplicación de la forma suprema que puede revestir el poder coactivo del Estado: la pena criminal. En consecuencia ocupa un lugar importante en el conjunto del ordenamiento, hasta el punto de que, no sin razón, al Código Penal se le ha considerado como una especie de "Constitución negativa".

Por todo ello, efectivamente, dicho Código ha de tutelar los valores y principios básicos de la convivencia social pero a la vez entendemos que debe ser respetuoso con el principio de intervención mínima que creemos debe informarlo.

Antes de iniciar el análisis del Código Penal vamos a restringir el dominio sobre el que actuaremos. Éste será tan sólo el que atañe a las nuevas tecnologías de la información y directamente a ellas, pues si hiciésemos una interpretación más amplia abarcaríamos prácticamente todo aquél. Así, por ejemplo, un homicidio, aunque sea realizado con ayuda de un ordenador, no lo consideramos objeto de nuestro análisis.

Una vez analizado el Código respecto a lo que aquí nos interesa, trataremos de estudiar los grandes grupos de ilícitos que contempla y así poder comprobar si es ya suficiente o sería conveniente proponer algún caso más, *de lege ferenda* (es decir, cambios legislativos),.

2. Análisis del Código Penal

Nos parece importante, entre las disposiciones generales, el artículo 26 que, aunque con una redacción poco afortunada, dentro del ámbito penal abre un futuro prometedor para el documento electrónico, figura que emerge cada día con más fuerza y que poco a poco va sustituyendo al papel, testigo durante muchos siglos de las relaciones jurídicas (la denominada Galaxia Von Neumann se está imponiendo a la Galaxia Gutenberg).

Art. 26. *"A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".*

Entendemos que esa referencia a todo soporte material, aunque incorrecta pues nunca un soporte es un documento sino el continente del mismo, puede incluir un soporte magnético o electrónico. Asimismo, las palabras 'expresar' o 'incorporar' permiten admitir la grabación informática o electrónica. A todo ello nos referiremos más adelante.

2.1. Delitos contra la intimidad

El Título X, "Delitos contra la intimidad, el derecho a la

propia imagen y la inviolabilidad del domicilio", dedica su Capítulo Primero, que comprende los **artículos 197** al **200**, al descubrimiento y revelación de secretos.

Este Capítulo, aparte de otras cosas, viene a regular en sede penal las infracciones que se cometan en el ámbito de la **Ley Orgánica 5/1992** de 29 de octubre de Tratamiento Automatizado de Datos de carácter personal (**LORTAD**).

Durante estos últimos años, desde que entró en vigor la LORTAD, venía sucediendo que al no estar recogidas en el antiguo Código Penal las sanciones correspondientes, se podía sancionar en vía administrativa, se podía solicitar una indemnización en vía civil, se podía recurrir por la vía contencioso-administrativa, pero no se podían castigar las infracciones más graves al no estar aquéllas tipificadas en el Código Penal. Esta situación ha cambiado y a partir de la entrada en vigor de la **Ley Orgánica 10/95** de 23 de noviembre, las infracciones que se cometan contra la LORTAD y que, por su gravedad, tengan carácter penal, pueden ser sancionadas.

Analicemos los artículos que figuran en este Capítulo, incluido el **artículo 200**, que, aunque referido a las personas jurídicas y por tanto fuera del ámbito de la LORTAD, resulta interesante contemplarlo por la importancia socioeconómica que puede tener.

Art. 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.*[1]
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 quién 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 afectan a los 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 impondrán 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 y 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 de prisión de cuatro a siete años".

En el punto 1 se contempla la figura de quien para descubrir los secretos o vulnerar la intimidad de otro se apodera de mensajes de correo electrónico[2] o cualesquiera otros documentos. Aquí entendemos que, a tenor de lo que dispone el **art. 26** de la Ley, se encuentra comprendido cualquier tipo de documento electrónico.

En el mismo punto también se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Pensamos que entre lo anterior se encuentra el llamado 'pinchado' de redes informáticas. Es importante advertir que en este punto no se habla para nada de datos de carácter personal ni de datos automatizados, a los que se refiere el mismo artículo en el punto siguiente, sino a secretos y a vulneración de la intimidad en general.

El punto 2 del artículo se refiere específicamente a datos de carácter personal pero abarcando no sólo, como actualmente hace la LORTAD, los ficheros informáticos, electrónicos o telemáticos, sino también los ficheros convencionales, a los que se refiere al hablar de "cualquier otro tipo de archivo o registro público o privado".

Se sanciona, ya referido a los datos de carácter personal o familiar, a quién sin estar autorizado:
a) en perjuicio de tercero: se apodere, utilice, modifique.
b) acceda por cualquier medio.
c) en perjuicio del titular de los datos o de un tercero: altere, utilice.

Las penas se agravarán si los datos se: difunden, revelan, ceden. Asimismo se sanciona a quien conociendo su origen ilícito y sin haber tomado parte en el descubrimiento: difunda, revela, ceda. El hecho de que quien cometa el delito sea encargado o responsable del fichero agrava la pena. Existen unas circunstancias agravantes, que se dan en función:
a) carácter de los datos: ideología, religión, creencias, salud, origen racial, vida sexual. Dichos datos son los que en la LORTAD se conocen como datos especialmente protegidos y comúnmente como datos sensibles.
b) Circunstancias de la víctima: menor de edad, incapaz. El hecho de que persiga un fin lucrativo igualmente eleva la pena.

Artículo 198. "La autoridad o funcionario 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".

La condición de autoridad o funcionario público lógicamente agrava las penas dada la situación de privilegio en que actúa.

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 meses.*

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".

En este artículo se contempla el secreto profesional, aplicable en muchos casos en el mundo informático.

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".*

Como decíamos no ha mucho[3], si a cualquier ciudadano ajeno al mundo del Derecho se le pregunta si las personas jurídicas tienen intimidad, la respuesta rotunda sería no, e inclusive quizás preguntase por qué se les llama personas. En la doctrina, el tema objeto de discusión es más amplio y lo que cabe preguntarse es si son titulares de derechos fundamentales las personas jurídicas.

Puede suceder que éstas se vean afectadas por conductas prohibidas por las normas que protegen la intimidad en las personas físicas y no gocen de un mecanismo adecuado para poder defenderse.

Esto supone, como dice Orozco Pardo, que la persona jurídica pase a ser titular de unos derechos y facultades, lo que por esencia no es posible, pero que, con el ánimo de impedir su indefensión, cabe extender la protección de la Ley a tales entidades. Así, el **Convenio 108 del Consejo de Europa** de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su artículo 1 se refiere sólo a las personas físicas pero en el artículo 3 b) deja abierta la posibilidad de que los Estados miembros puedan extender el régimen de protección a las personas jurídicas.

La Ley portuguesa de protección de datos, en su artículo 3.1 b), dice que también son titulares de derechos las personas jurídicas, siempre que los ficheros, bases o bancos de datos contengan datos personales. También protegen a las personas jurídicas las leyes francesa, danesa y luxemburguesa.

El procedimiento a seguir por los delitos que figuran anteriormente se señala en el **artículo 201**.

Art. 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 4º del artículo 130".[4]

2.2. Delitos contra el patrimonio

Los delitos contra el patrimonio y contra el orden socioeconómico figuran en el Título XIII.

El concepto de 'llave'. Es importante, en el dominio en que nos movemos, la mención a 'llave' que figura en el **artículo 239**.

Art. 239. *Se considerarán llaves falsas:*
1. Las ganzúas u otros instrumentos análogos.
2. Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3. Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia".

Así las tarjetas magnéticas sustraídas a sus propietarios se considerarán llaves falsas. Es importante esta consideración en relación con el **artículo 238**, en el que para calificar un delito de robo con fuerza en las cosas es necesario que concurra alguna de varias circunstancias, entre las que se encuentra el uso de llaves falsas.

La estafa informática. En el pasado reciente se ha tratado, con poco éxito, de reconducir el fraude informático hacia la figura de la estafa. El Código Penal de forma explícita lo hace figurar en el punto e del **artículo 248**.

Art. 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".

La estafa se puede definir[5] como el perjuicio patrimonial realizado con ánimo de lucro mediante engaño. El engaño es elemento necesario de este delito. Consiste, según Cuello Calón, en aprovecharse del error provocado o mantenido por el agente en la persona engañada.

Hasta la entrada en vigor del nuevo Código Penal ha sido difícil reconducir determinados fraudes informáticos debido a la inexistencia del elemento de engaño a una persona. Prueba de que tenían razón los que se oponían a la aceptación de aquellos como estafas ha sido la necesidad de incluir un nuevo punto en el que específicamente se refiere a la manipulación informática en el artículo en el que se regula la estafa.

No vamos a entrar aquí en la discusión doctrinal sobre si una manipulación informática de las características de las que señala el punto 2 del **artículo 248** reúne los elementos constitutivos de la figura de estafa. A efectos prácticos basta con que figure como tal en el Código Penal.

El Capítulo VI está dedicado a las defraudaciones y dentro de él la Sección 3ª a las defraudaciones de fluido eléctrico y análogas. Dentro de estas últimas aparece el uso ilícito de un equipo terminal de telecomunicaciones.

Artículo 256. *"El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas será castigado con la pena de multa de tres a doce meses".*

Se considera defraudación el uso, sin consentimiento de su titular, de cualquier equipo terminal de telecomunicación.

Daños a materiales informáticos. El Capítulo IX está dedicado a los daños.

Art. 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:*
2) 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".

En las situaciones contempladas en este artículo se pueden incluir los famosos virus informáticos y los piratas informáticos o *hackers*.

Propiedad intelectual e industrial. Los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores se contemplan en el Capítulo IX.

Art. 270. *"Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quién, 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 transporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios".*

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador".

El **artículo 10** del **Texto Refundido de la Propiedad Intelectual** señala que 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 según el apartado i) los programas de ordenador.

En el **artículo 270** se contemplan los siguientes casos:
a) quien con ánimo de lucro y en perjuicio de tercero: reproduzca, plagie, distribuya, comunique públicamente.
b) sin autorización del titular: transforme.
c) intencionadamente sin autorización: importe, exporte, almacene.
d) medios específicamente destinados a facilitar la supresión no autorizada o neutralización de dispositivo de protección: fabricación, puesta en circulación, tenencia.

Es interesante advertir que no sólo se sanciona la fabricación o puesta en circulación sino la simple tenencia de un dispositivo para saltarse las llaves lógicas o las famosas 'mochilas'. La sanción es de pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses.

Art. 271. *"Se impondrá la pena de prisión de un año a cuatro años, multa de ocho a veinticuatro 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 el daño causado revista especial gravedad.
En tales casos, el Juez o Tribunal podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. El cierre temporal no podrá exceder de cinco años.

Si el beneficio obtenido es cuantioso o el daño causado es grave se elevan las penas y además se inhabilita al autor del delito para el ejercicio de la profesión relacionada con el delito cometido".

Art. 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 la 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 periódico oficial".

Según lo dispuesto en la Disposición final 6ª este artículo tiene carácter de Ley ordinaria, lo que puede facilitar, en su día, su modificación o supresión si ello fuere necesario.

Estos artículos son, en sede penal, la respuesta a esa lacra de nuestro tiempo que es la piratería informática. Ésta resulta muy dañina para el desarrollo informático pero entendemos que sólo con la amenaza de una sanción penal no se soluciona el problema. Es necesaria una labor educativa pues hasta que no hayamos convencido al infractor que cuando está copiando un programa de ordenador es como si estuviese robando la cartera a otra persona difícilmente se hallará solución. Insistimos, resulta vital esa labor educativa.

La propiedad industrial se encuentra protegida en la Sección 3ª del mismo Capítulo.

Art. 273. *"Será castigado con las penas de prisión de seis meses a dos años y multa de seis a veinticuatro meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.*
2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.
3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía en un producto semiconductor".

El derecho de patentes protege los inventos y como tal hemos de entender los productos robóticos. Los programas de ordenador fueron exceptuados de esa protección. Ahora bien, cuando un programa de ordenador forma parte de un robot, la patente que protege a éste protegerá también a aquél. De esta forma en algunos casos un programa de ordenador puede estar protegido por la propiedad industrial y al mismo tiempo por la propiedad intelectual.

Artículo 276.1. *"Se impondrá la pena de prisión de dos a cuatro años, multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando los delitos tipificados en los anteriores artículos revistan especial gravedad, atendiendo al valor de los objetos producidos ilícitamente o a la especial importancia de los perjuicios causados.*
2. En dicho supuesto, el Juez podrá decretar el cierre temporal o definitivo de la industria o del establecimiento condenado. El cierre temporal no podrá exceder de cinco años".

De igual forma que en otros casos anteriores ya examinados las circunstancias: valor y perjuicio elevan la pena.

La importancia de los secretos empresariales, fruto muchas veces de largos años de trabajo e investigación, se protegen en la Sección 3ª del mismo Título.

Artículo 278. *"El que para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.*
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

En este artículo, dedicado a sancionar a quien se apodere, difunda, revele o ceda secretos empresariales, entre los posibles objetos de apoderamiento se encuentran los documentos electrónicos y los soportes informáticos, algo no habitual en el Código anterior.

"Si el secreto se utilizare en provecho propio, las penas se impondrán en su mitad inferior".

Artículo 279. *"La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quién tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.*

La persona obligada legal o contractualmente a guardar el secreto si lo difundiere, revelare o cediere será sancionada con la pena fijada en el artículo anterior. La pena será reducida si se utiliza el secreto en provecho propio".

Art. 280. *"El que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses".*

Igualmente se sanciona a quién se aproveche de alguna forma, revelare, difundiere o cediere los secretos empresariales obtenidos aunque no hubiese participado en su consecución.

2.3. Delitos de falsedades

Las falsedades se contemplan en el Título XVIII del Código. La asimilación que hace el **artículo 387** de las tarjetas de débito y de crédito a la moneda es muy importante de cara a la defensa de éstas frente al ataque criminal de que están siendo objeto.

Art. 386. *"Será castigado con las penas de prisión de ocho a doce años y multa del tanto al décuplo del valor aparente de la moneda:*
1º El que fabrique moneda falsa.
2º El que la introduzca en el país.
3º El que la expenda o distribuya en connivencia con los falsificadores o introductores.

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 las penas de arresto de nueve a quince fines de semana y multa de seis a veinticuatro meses, si el valor aparente de la moneda fuera superior a cincuenta mil pesetas".

Art. 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 monedas las tarjetas de crédito, las de débito y los cheques de viaje. Igualmente se*

equipararán a la moneda nacional, las de la Unión Europea y las extranjeras".

El dinero de plástico, como vulgarmente se le conoce, tiene una gran incidencia en el tráfico comercial y financiero de nuestro tiempo. Así, por ejemplo, la cantidad que anualmente se maneja en nuestro país a través de las tarjetas de crédito y débito supera los siete billones de pesetas.

Un mercado así debía estar perfectamente regulado por el Derecho. Sin embargo no es así a pesar de las promesas del Ejecutivo en diferentes ocasiones acerca de su regulación.

En este artículo, asemejando las tarjetas, tanto de débito como de crédito, a la moneda falsa, se sanciona su falsificación y puesta en circulación. No debemos olvidar que la fabricación de las tarjetas es un negocio floreciente y en auge creciente.

A la falsificación de los documentos públicos oficiales y mercantiles y de los despachos transmitidos por los servicios de telecomunicación se dedica la Sección 1ª del Capítulo II de este Título.

Art. 390. *"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:*
1º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.
2º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.
3º 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.
4º 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".

Como decíamos al principio el **artículo 26** del Código al considerar documento todo soporte material que exprese o incorpore datos a los efectos del mismo, permite que cualquier artículo del Código que se refiera a un documento pueda ser aplicado a éste aunque sea electrónico.

El **artículo 38 de la Ley 30/1992** de 26 de noviembre del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su punto 3 ordena que "*todos los registros generales así como todos los registros que las Administraciones Públicas, establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos, deberán instalarse en soporte informático".*

El sistema informático deberá garantizar la integración informática en el registro general de las anotaciones efectuadas en los restantes registros del órgano administrativo. *"Mediante convenios de colaboración suscritos entre las Administraciones Públicas se establecerán los sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos".*

Como se ve, las Administraciones Públicas tratan de incorporarse a las nuevas tecnologías de la información y más aún según lo dispuesto en los **artículos 45** y **46** de la citada **Ley 30/92**.

Vemos pues que, aunque con las necesarias cautelas y a la espera del correspondiente desarrollo reglamentario, el documento electrónico es válido y tiene eficacia en el ámbito de las Administraciones Públicas; por lo tanto, lo que contiene el **artículo 390** y siguientes es aplicable al documento electrónico.

Art. 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".*

En este artículo se sanciona no ya a la autoridad o funcionario público que cometa la falsedad sino también al que fuese imprudente y a causa de esa imprudencia se cometiese alguna falsedad de las previstas en el artículo anterior.

Art. 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".*

La sanción se extiende en este caso a las falsedades cometidas por un particular en un documento público.

Art. 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".*

La utilización del documento falso se sanciona aunque con una pena inferior a la de los falsificadores.

Art. 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.
En la sanción se contempla tanto a los funcionarios autores de la falsedad del documento como a quien conocedor de la falsificación se aprovecha de ello".

Art. 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".*

Aquí se traslada al ámbito privado el delito por alteración o simulación de un documento, suposición de la intervención en un acto de personas que no han asistido o atribución de declaraciones o manifestaciones que no han efectuado.

Art. 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".*

La simple posesión, no sólo su creación, de un programa de ordenador destinado a las falsificaciones a que nos hemos referido en los artículos anteriores será sancionada de igual forma que la que figura para los autores.

2.4. Delitos contra la Administración Pública

Art. 413.*" La autoridad o funcionario público que, a sabien-das, sustrajere, destruyere, inutilizare u ocultare, total o parcialmente, documentos cuya custodia le está encomendada por razón de su cargo, incurrirá en las penas de prisión de uno a cuatro años, multa de siete a veinticuatro meses, e inhabilitación especial para empleo o cargo público por tiempo de tres a seis años".*

Art. 414. *"1) A la autoridad o funcionario público que por razón de su cargo, tenga encomendada la custodia de documentos respecto de los que la autoridad competente haya restringido el acceso, y que a sabiendas destruya o inutilice los medios puestos para impedir ese acceso o consienta su destrucción o inutilización incurrirá en la pena de prisión de seis meses a un año o multa de seis a veinticuatro meses y, en cualquier caso, inhabilitación especial para empleo o cargo público por tiempo de uno a tres años.*
2) El particular que destruyere o inutilizare los medios a que se refiere el apartado anterior, será castigado con la pena de multa de seis a dieciocho meses".

Art. 415. *"La autoridad o funcionario público no comprendido en el artículo anterior que, a sabiendas y sin la debida autorización, accediera o permitiera acceder a documentos secretos cuya custodia le está confiada por razón de su cargo, incurrirá en la pena de multa de seis a doce meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años".*

Art. 416. *"Serán castigados con las penas de prisión o multa inmediatamente inferiores a las respectivamente señaladas en los tres artículos anteriores los particulares encargados accidentalmente del despacho o custodia de documentos, por comisión del Gobierno o de las autoridades o funcionarios públicos a quienes hayan sido confiados por razón de su cargo, que incurran en las conductas descritos en los mismos".*

Los **artículos 413** a **415** contemplan la infidelidad en la custodia de documentos públicos tanto por autoridades o funcionarios como por particulares cuando estos accidentalmente tengan el deber de custodia.

2.5. Otros delitos y faltas

Art. 536. *"La autoridad, funcionario público o agente de estos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.*

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses".

La interceptación de señales de comunicación, que puede ser comunicación entre ordenadores, que realice una autoridad o funcionario es sancionada, agravándose la pena si dicha información se divulga o revela.

Art. 623. *"Serán castigados con arresto de dos a seis fines de semana o multa de uno a dos meses...*
... 4) Los que cometan estafa, apropiación indebida o defraudación de electricidad, gas, agua u otro elemento, energía o fluido o en equipos de telecomunicación en cuantía no superior a cincuenta mil pesetas".

Art. 625. *"1) Serán castigados con la pena de arresto de uno a seis fines de semana o multa de uno a veinte días los que intencionadamente causaren daño cuyo importe no exceda de cincuenta mil pesetas.*
2) Se impondrá la pena en su mitad superior si los daños se causaran en bienes de valor histórico, artístico, cultural o monumental".

Art. 629. *"Serán castigados con la pena de arresto de uno a cuatro fines de semana o multa de quince a sesenta días, los que, habiendo recibido de buena fe moneda, billetes, sellos de correos o efectos timbrados falsos, los expendieren en cantidad que no exceda de cincuenta mil pesetas, a sabiendas de su falsedad".*

Estos artículos del Libro III se refieren a faltas y se corresponden con los ya vistos salvo en la cuantía, que no excede de cincuenta mil pesetas.

4. Síntesis de lo analizado

Según Cuello Calón[6], el delito es un acto humano, antijurídico, culpable y sancionado con una pena. El Código Penal castiga los delitos con penas graves y menos graves en su artículo 13 puntos 1 y 2. El punto 3 de dicho artículo señala que son faltas las infracciones que la Ley castiga con pena leve.

Delito informático, según Davara Rodríguez[7] se puede definir como: "*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*".

La selección en función de un concepto de ciertas partes de un todo, especialmente en el campo jurídico, conlleva una gran carga de subjetividad, algo de lo que por supuesto somos conscientes y por tanto asumimos.

Entendemos que el Código Penal contempla el delito informático en los siguientes artículos:

1. Delitos contra la intimidad (arts. 197, 198 y 199)
2. Delitos contra el patrimonio
2.1 Estafas (art. 248)
2.2 Defraudaciones (art. 256)
2.3 Daños (art. 264)
2.4 Propiedad intelectual (arts. 270, 271 y 272)
2.5 Propiedad industrial (arts. 273 y 276)
2.6 Secreto empresarial (arts. 278, 279 y 280)
3. Delitos de falsedades
3.1 Falsedad en documento público (arts. 386, 387, 390, 391, 392, 393, 394 y 400)
3.2 Falsedad en documento privado (arts. 395, 396 y 400)
4. Delitos contra la Administración Pública
4.1 Infidelidad en la custodia de documentos públicos (arts. 413,414,415416)
5. Otros delitos y faltas
5.1 Interceptación de comunicaciones (art. 536)
5.2 Faltas (arts. 623, 625 y 629)

El Código Penal vigente supone un paso hacia adelante en el lento caminar hacia la regulación penal del Derecho Informático.

Queda mucho camino por recorrer y eso lo veremos cuando los Jueces y Tribunales se tengan que enfrentar a hechos corrientes en el mundo informático y tengan que calificarlos de una u otra forma.

Importante es el **artículo 26** con su admisión como documento no sólo del papel, símbolo de la cultura de una época sino cualquier otro soporte siempre que pueda expresar o incorporar datos, hechos o narraciones y que tenga eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Los artículos correspondientes al derecho contra la intimidad eliminarán esa laguna existente en nuestro derecho penal desde la entrada en vigor de la **Ley Orgánica 5/1992** de 29 de octubre de **Regulación del Tratamiento Automatizado de Datos** de carácter personal.

La figura de la estafa informática, incorporada al punto 2 del **artículo 248**, sanciona una gran parte de lo que se venía conociendo como fraude informático.

La figura del pirata informático o *hacker* puede estar comprendida según los casos en los **artículos 197** (derecho a la intimidad), **264** (daños) y **278** (secreto empresarial).

El virus, aún el más benigno, puede incluirse entre el delito de daños del **artículo 264.2** al considerarse que altera los datos o los programas.

Para terminar quisiéramos decir que en cualquier caso el Código Penal debe responder al principio de mínima intervención y muchas de las situaciones irregulares que se presentan en el transcurrir informático no precisan tener cabida en el Código Penal pudiendo resolverse por los otros sistemas que el ordenamiento jurídico facilita al perjudicado para la defensa de sus intereses.

Notas

[1] **Artículo 50.** 1. La Pena de multa consistirá en la imposición al condenado de una sanción pecuniaria.
2. La pena de multa se impondrá, salvo que la Ley disponga otra cosa, por el sistema de días-multa.
3. Su extensión mínima será de cinco días, y la máxima de dos años. Este límite máximo no será de aplicación cuando la multa se imponga como sustitutiva de otra pena; en este caso su duración será la que resulte de la aplicación de las reglas previstas en el artículo 88.
4. La cuota diaria tendrá un mínimo de doscientas pesetas y un máximo de cincuenta mil. A efectos de cómputo, cuando se fije la duración por meses o por años, se entenderá que los meses son de treinta días y los años de trescientos sesenta.
5. Los Jueces o Tribunales determinarán motivadamente la extensión de la pena dentro de los límites establecidos para cada delito y según las reglas del Capítulo II de este Título. Igualmente, fijarán en la sentencia, el importe de estas cuotas, teniendo en cuenta para ello, exclusivamente la situación económica del reo, deducida de su patrimonio, ingresos, obligaciones y cargas familiares y demás circunstancias personales del mismo.
6. El Tribunal determinará en la sentencia el tiempo y forma del pago de las cuotas.

Artículo 51. Si, después de la sentencia, el penado empeorare su fortuna, el Juez o Tribunal excepcionalmente y tras la debida indagación de la capacidad económica de aquél, podrá reducir el importe de las cuotas.

[2] La incorporación de los mensajes electrónicos al elenco de bienes protegidos se hizo como consecuencia de una propuesta presentada a los diversos Grupos Parlamentarios por la **CLI** (**Comisión de Libertades e Informática**), por indicación de ATI, que formaba parte de dicha organización.

[3]. **Peso Navarro, Emilio del y Ramos González, Miguel Ángel;** *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*. Díaz de Santos. Madrid 1994 pág. 67.

[4] **Artículo 130.4** Por el perdón del ofendido, cuando la Ley así lo prevea. El perdón habrá de ser otorgado de forma expresa antes de que se haya iniciado la ejecución de la pena impuesta. A tal efecto, declarada la firmeza de la sentencia, el Juez o Tribunal sentenciador oirá al ofendido por el delito antes de ordenar la ejecución de la pena.

[5] **Eugenio Cuello Calón.** *Derecho Penal*. Tomo II (Parte Especial; Volumen segundo). Bosch. Barcelona, 1972, pág. 914.

[6] **Eugenio Cuello Calón;** *Derecho Penal*. Tomo I (Parte General). Volumen Primero, pág. 285.

[7] **Miguel Ángel Davara Rodríguez;** *Derecho informático*. Aranzadi. Pamplona, 1993.

LegisTIC

Protección del Software y de la Propiedad intelectual

Jorge Páez Mañá
Doctor en Derecho, CINDOC-CSIC

1.Introducción

Los continuos y a menudo vertiginosos avances producidos en la actual sociedad tecnológica de la información, en virtud de la aplicación de las nuevas tecnologías informáticas, han provocado un cambio sustancial en la evolución de los mercados nacionales e internacionales de bienes y servicios.

La interrelación de redes regionales de telecomunicación y la normalización de los protocolos de comunicación han permitido conformar una red mundial que posibilita la difusión de contenidos digitales en unos volúmenes impensables hace tan solo unas décadas.

La expansión de la demanda estimulada por la mejora de la infraestructura de la red, el incremento de la multiplicidad de productos y servicios basados en la tecnología informática y los avances del hardware y software, ha generado un crecimiento espectacular de este sector del mercado que, en lo que se refiere a los programas informáticos, presenta una ratio, en los países más desarrollados, diez veces superior a la media.

A fin de consolidar y proteger la industria informática del software, que esta sustentada en la comercialización de unos bienes inmateriales de fácil reproducción, manipulación y transmisión, se ha hecho preciso establecer, en una forma nítida, un específico régimen jurídico protector de los derechos relacionados con la elaboración, comercialización y uso de los programas de ordenador, a tenor de los intereses de los autores y las compañías que los comercializan, y de las necesidades de los usuarios y de la sociedad en general.

Dada la consolidada internacionalización de este sector del mercado, su regulación jurídica ha precisado de una armonización de los marcos normativos aplicables a los programas establecidos en las legislaciones nacionales y supranacionales.

En nuestro país, la regulación jurídica de este fenómeno se encuentra en el **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 armonizándolas disposiciones legales vigentes sobre la materia; los artículos 428 y 429 del **Código Civil**, que remiten a lo legislado en la citada Ley de Propiedad Intelectual, quedando como subsidiario lo estipulado en el mismo sobre la propiedad respecto a lo no regulado en dicha Ley; y los artículos 270, 271 y 272 del Código Penal respecto a los delitos relativos a la propiedad intelectual (reproducción ilegal, plagio, distribución no autorizada, comunicación publica ilícita, transformación no consentida de obras, importación o exportación ilegal de obras, etc.).

El texto refundido recoge y actualiza lo anteriormente regulado, entre otras, por las **leyes 22/1987**, de 11 de noviembre, de propiedad intelectual; **20/1992**, de 7 de julio, de modificación de la **Ley 22/1987**, de propiedad intelectual; **16/1993**, de 23 de diciembre, de incorporación al derecho español de la Directiva sobre la protección jurídica de programas de ordenador; **43/1994**, de 30 de diciembre, de incorporación al derecho español de la Directiva sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual; y **27/1995**, de 11 de octubre, de incorporación al derecho español de la Directiva relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines.

El **Código Civil** se aplica como norma subsidiaria reguladora de los aspectos civilistas (propiedad, contratos, responsabilidad extracontractual, etc.). Asimismo el Código Penal se aplica como norma reguladora de la responsabilidad penal derivada de los actos ilícitos relacionados con la propiedad intelectual.

En el ámbito comunitario son aplicables las **directivas 91/250/CEE** sobre la protección jurídica de programas de ordenador; **92/100/CEE** sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual; **93/98/CEE** relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines, todas ellas recogidas, en cuanto a lo estipulado en sus preceptos, en el Texto refundido de la ley de propiedad intelectual, anteriormente citado.

A nivel internacional su regulación esta integrada en el **Convenio de Berna** para la protección de las obras literarias y artísticas revisado en París el 24 de julio de 1971 y el Acuerdo por el que se establece la Organización mundial del comercio y acuerdos anejos (Anexo 1C: Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio) hecho en Marrakech el 15 de abril de 1994.

Esta prolija producción normativa pone aun más de manifiesto la importancia económica y cultural del desarrollo informático generado por las creaciones intelectuales de los programadores y la necesidad de dotar de un régimen jurídico de protección, debidamente estructurado a nivel nacional, regional y mundial, que sirva de salvaguardia de los derechos afectados por el mismo, que permita su normal evolución en condiciones normales de lícita competencia profesional y comercial.

A efectos de delimitar las repercusiones jurídicas de los actos relacionados con la producción, comercialización y uso de los programas de ordenador se hace preciso analizar las condiciones que se requieren para que estos puedan ser considerados objeto de protección jurídica, los aspectos relacionados con su autoría y titularidad, la delimitación de los derechos y obligaciones de sus autores y usuarios, la forma y modo de transmisión de dichos derechos y los medios de protección jurídica establecidos como garantía de los múltiples intereses en juego.

2. Condiciones para la protección jurídica

La protección jurídica del software se extiende a diferentes productos, susceptibles de acceder a la misma, cuando reúnan determinadas condiciones estipuladas en los correspondientes corpora normativos.

El producto genuino de protección del software es el programa de ordenador, entendido este como secuencia de instrucciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar alguna tarea determinada o para obtener algún resultado concreto. Dado que los programas se protegen con independencia de su forma de expresión y fijación deberán entenderse como protegidos tanto el código fuente como el código objeto de los mismos.

Deberán entenderse como susceptibles de protección el software de arranque o programas internos fijos, el software del sistema operativo o programas básicos funcionales y el software de desarrollo o programas de aplicación. Esta protección cubrirá tanto los programas originales como a las sucesivas versiones de los mismos y a los programas derivados siempre y cuando cumplan las condiciones exigibles para acceder a dicha protección.

Respecto a las partes de cualesquiera de los programas cuya función sea la de servir de enlace o interface entre los diferentes componentes de software y/o hardware deberán igualmente considerarse como objeto protegible en la misma forma y condiciones que el resto del software.

Junto a estos productos genuinos son protegibles, como forma de expresión de las ideas contenidas en los dichos programas, la documentación preparatoria de los mismos. Por último es igualmente protegible la documentación técnica y los manuales de uso de los programas.

Para acceder a la protección jurídica otorgada por la legislación sobre propiedad intelectual se precisa únicamente que las obras objeto de protección, ya sean programas, documentación preparatoria o técnica, o manuales de uso, sean creaciones intelectuales originales. Así pues es indiferente, a efectos legales, la calidad de los programas o documentación complementaria e incluso la novedosidad que representan en cuanto a las ideas contenidas en los mismos. Por el contrario, no son susceptibles de protección jurídica las ideas y principios en los que se basan los programas, incluidos los que sirven de fundamento a sus interfaces.

De lo antedicho se deriva que las ideas y principios integrados en los desarrollos lógicos, algoritmos y lenguajes de programación no están protegidos jurídicamente pudiendo ser utilizados como elementos de base de otros programas que, incluso con la misma finalidad, establezcan diferentes concepciones y formas de lograr un similar objetivo. Tampoco se admite el acceso a la protección jurídica de aquellos programas cuya finalidad sea la de ocasionar efectos nocivos a los sistemas informáticos (virus informáticos y similares), con independencia de las responsabilidades civiles y penales que, de la producción de los mismos, pudieran derivarse.

3. Autoría y Titularidad

En los diferentes cuerpos jurídicos, nacionales e internacionales, puede observarse el reconocimiento de la existencia de un nexo de unión entre las obras objeto de propiedad intelectual y sus creadores. En dichos cuerpos se suele estipular que, para que una obra pueda quedar incluida en el ámbito de protección de las legislaciones sobre propiedad intelectual, ésta deberá haber sido producida en virtud de una actividad intelectual genuina, y por ende original, de sus creadores, que reciben la consideración de autores de la misma.

Los autores deberían ser necesariamente personas naturales ó físicas, ya que solamente dichos sujetos pueden realizar una actividad intelectual susceptible, en virtud de su propia e íntima idiosincrasia, de crear obras originales que reflejen sus personales conocimientos, ideas, elucubraciones o sentimientos, tal y como se pone de manifiesto en la parte general del Texto refundido de nuestra ley de propiedad intelectual. Sin embargo algunas legislaciones permiten otorgar la condición de autor, en determinados casos, a las personas jurídicas (sociedades, empresas, asociaciones, etc.), en función de la iniciativa empresarial generada en el seno de las mismas, con objeto de proteger la explotación comercial del producto resultante.

Esta seudoautoría debería entenderse únicamente como una forma de reconocimiento de que los derechos de explotación en exclusiva de las obras, publicadas bajo el nombre de dichas personas jurídicas, corresponden *ab initio* a las mismas, en virtud del precepto legal que regula dichos supuestos, debiendo evitarse cualquier otra interpretación que desvirtúe el vínculo establecido entre la obra y su creador (la persona física que la genera mediante su actividad intelectual).

Esta especial circunstancia ha provocado que tanto en la Directiva de protección jurídica de los programas de ordenador, como en la parte específica del Texto refundido de nuestra ley de propiedad intelectual se exceptue de la regla general, que considera autores únicamente a las personas físicas, a los autores de las obras colectivas y, más explícitamente, a los autores de los programas de ordenador que pudieran considerarse obras colectivas. Así pues, a efectos jurídicos, en los programas de ordenador realizados por un único programador, éste será considerado como su autor.

En cuanto a los programas desarrollados mediante la participación de diferentes programadores, la autoría de los mismos presenta las siguientes particularidades:

- En los "programas de ordenador en colaboración" creados mediante el esfuerzo unitario de varios programadores, que sean resultado unitario de la contribución común, serán considerados, todos ellos, como coautores.
- En los "programas de ordenador colectivos", creados por iniciativa y bajo la coordinación de una persona natural o jurídica, constituidos por la fusión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual han sido concebidos, tendrá la consideración de autor, salvo pacto en contrario, la persona física o jurídica que lo edite y divulgue bajo su nombre.
- En los "programas de ordenador compuestos" que incorporen otros programas preexistentes que constituyan creaciones autónomas, sin la colaboración de los autores de estos últimos, se establece una doble autoría: la primera recaerá sobre el creador del programa maestro en el que se incluye el incorporado, y la segunda sobre el creador de este último, que se considera independiente y autónoma de la primera.
- Los titulares de los programas ostentan la tenencia en exclusiva de la propiedad de los mismos, pudiendo reivindicar su dominio, poseerlos, usarlos, divulgarlos, comercializarlos, cederlos, modificarlos, reproducirlos o disponer de ellos en la forma que consideren más conveniente sin más límites que los establecidos en la ley.
- Se considerarán como titulares de los programas a la persona o grupo de personas físicas o jurídicas que adquieran los derechos de propiedad de sus autores o de aquellos a quienes estos la hubieran transmitido.
- En los programas desarrollados de forma unipersonal, la titularidad *ab initio* de los mismos recaerá en sus creadores individuales.

La titularidad *ab initio* de los programas en colaboración corresponderá conjuntamente a todos ellos. Los derechos patrimoniales derivados de dicha titularidad les corresponderán en la proporción que determinen, si bien se permite que cada uno pueda realizar una explotación separada de su aportación. Para la divulgación o modificación de estos programas se precisará del consentimiento común, no pudiendo oponerse injustificadamente ningún coautor a su explotación, una vez producida la divulgación del mismo.

La titularidad *ab initio* de los programas creados como obra colectiva corresponderá, salvo pacto en contrario, a la persona física o jurídica que los edite o divulgue bajo su nombre. Los programadores partícipes en la obra colectiva no podrán oponerse a que ésta se divulgue bajo el nombre de su titular.

La titularidad *ab initio* de los programas de ordenador compuestos corresponderá al autor de los mismos, perviviendo junto a dicha titularidad, los derechos de propiedad de los programas independientes incorporados que permanecen en poder sus titulares. El titular de los programas compuestos debe tener muy presente que, para su producción, deberá contar con la autorización de los titulares de los programas incorporados en forma previa a su inclusión como parte del programa compuesto.

El ejercicio de los derechos de explotación, por el titular de este tipo de programas, deberá ejercerse sin perjuicio de los derechos de los titulares de los programas incorporados, siendo compatibles e independientes los derechos sobre el programa compuesto y los derechos sobre los programas independientes incluidos en el mismo.

La titularidad *ab initio* de los programas creados por los trabajadores asalariados, en el ejercicio de sus funciones o siguiendo las instrucciones de su empresario, será ostentada por el empleador o el empleado a tenor de lo pactado en el contrato. A falta de pacto, se presumirá que la titularidad ha sido enteramente y en exclusiva transmitida al empresario.

Corresponde a los titulares de los programas de ordenador, siempre y cuando éstos constituyan obras consideradas como objetos de propiedad intelectual, el ejercicio exclusivo de los derechos de explotación en cualquier forma y lugar, y en especial los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser ejecutados sin su autorización salvo en los casos expresamente previstos en la legislación sobre propiedad intelectual.

Estos derechos pueden ser enajenados o transmitidos en forma total o parcial a sucesivos titulares, inter vivos o mortis causa, en cualesquiera de las formas admitidas en Derecho, ostentando los nuevos titulares los derechos así obtenidos.

4. Derechos de autor

El contenido de los derechos de Propiedad Intelectual está circunscrito a dos haces de derechos, los derechos morales y los derechos patrimoniales.

Entre los derechos morales reconocidos a los autores, que se consideran irrenunciables, inembargables, imprescriptibles e inalienables, se encuentran los de decidir sobre el momento y forma de divulgación de sus obras; indicar con su nombre o seudónimo la autoría de las obras o publicar anónimamente las mismas; exigir el reconocimiento de su autoría; modificar la obra, o retirarla del comercio por cambio de convicciones, respetando los derechos adquiridos por terceros; exigir el respeto a la integridad de la obra; y acceder al ejemplar único o raro de sus obras para ejercer los derechos de divulgación de las mismas previa indemnización de los perjuicios que pudiera con ello ocasionar.

Cabe destacar la condición de irrenunciabilidad de estos derechos, que implica que cualquier cesión de los mismos debe considerarse como nula y no aplicable.

Entre los derechos patrimoniales básicos, que se otorgan a los autores en forma exclusiva respecto a la explotación de sus obras, se encuentran los de reproducción, que abarca cualquier fijación de los programas, en forma total o parcial, incluso para uso personal, en forma permanente o transitoria, en un medio tal que permita su comunicación o la obtención de copias de la totalidad o parte de ellos; distribución, que incluye cualquier puesta a disposición del público del original o copias de los programas mediante su venta, alquiler, préstamo o cualquier otra forma; comunicación pública, que abarca cualquier acto, que exceda del ámbito estrictamente doméstico, que permita a una pluralidad de personas el acceso a los programas sin una previa distribución de los mismos; y transformación, que comprende la traducción a otro lenguaje de programación, adaptación, arreglo y cualquier otra modificación de los programas de la que se deriven obras diferentes, así como la reproducción de los resultados de tales actos.

Cuando se produzca la cesión del derecho de uso de los programas, se entenderá, salvo pacto en contrario, que dicha cesión tiene el carácter de intransferible y no exclusiva, presumiéndose que lo es para satisfacer únicamente las necesidades del usuario.

Los derechos patrimoniales se mantendrán, cuando el autor sea una persona física, durante toda su vida y setenta años después de su muerte o declaración de fallecimiento, pasando a dominio público tras dicho plazo, pudiendo a partir de ese momento ser utilizados los programas por cualquiera siempre que se respeten los derechos morales que se mantienen inalterables. Cuando el autor sea una persona jurídica la duración los derechos patrimoniales se mantendrá durante los setenta años siguientes a su licita divulgación o, caso de no haberse divulgado, al momento de su creación.

5. Derechos de los usuarios

Los usuarios legítimos de los programas de ordenador ostentarán por el hecho de la cesión lícita de uso de los mismos los siguientes derechos:

- El derecho a reproducir y transformar los programas adquiridos, incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización de los mismos a tenor de su finalidad.
- El derecho a realizar una copia de seguridad de los programas.
- El derecho a reproducir el código y a la traducción o adaptación de la forma del programa cuando dichos actos sean indispensables para obtener la información necesaria para la interoperatividad del programa, siempre y cuando dicha información no haya sido puesta a su disposición y se utilice únicamente para conseguir dicha interoperatividad.
- El derecho a obtener una información veraz, eficaz y suficiente sobre las características esenciales de los programas así como sobre las instrucciones o indicaciones para su correcto uso, junto con las advertencias y riesgos que pudieran derivarse de su utilización.
- El derecho de saneamiento de los vicios o defectos ocultos que tuviere el programa de ordenador.

Caso de pactarse la no responsabilidad del titular del programa por los vicios o defectos que pudieran descubrirse en el mismo, decaerá este derecho de saneamiento a no ser que

dicho titular tuviera conocimiento del mismo y no se lo hubiera comunicado, de forma fehaciente, a los usuarios, en cuyo caso sería nulo dicho pacto.
- El derecho a ser indemnizado por los daños que pudiera haberle ocasionado la utilización, conforme a las instrucciones de uso, del programa de ordenador suministrado por el cesionario.

Por su parte los usuarios que hubieren adquirido junto con el derecho de uso de los programas, la cesión de los derechos de explotación relacionados con ellos, podrán realizar tanto versiones sucesivas de los programas objeto de dicha cesión, como programas derivados de los mismos.

6. Transmisión de los derechos de explotación

Los derechos patrimoniales de autor, respecto a sus obras, pueden ser transmitidos por sus titulares por cualquier medio admitido en Derecho. En cualquier caso conviene tener presente los siguientes aspectos:
- La transmisión de los derechos de explotación de las obras queda limitada a las modalidades de explotación expresamente previstas, lo que conviene tener en cuenta, dada la independencia de los diferentes derechos de explotación (reproducción, distribución, comunicación pública, transformación, etc.) a fin de evitar creer que ha sido transmitido cualesquiera de dichos derechos con la sola cita de otro.
- No se considera admisible en derecho, la cesión del conjunto de obras que el autor pueda crear en el futuro, ni la explotación de las mismas por medios inexistentes en el momento de formalizar el contrato de cesión.
- Toda cesión de derechos deberá formalizarse por escrito si el autor así lo solicitase, no pudiéndose el cesionario negarse a ello so pena de permitir al autor la rescisión del contrato no formalizado en el momento en que éste así lo estimase conveniente.
- Las cesiones a título oneroso, otorgan al autor el derecho a percibir una participación proporcional a los ingresos obtenidos en la explotación de su obra en la cuantía convenida con el cesionario, pudiéndose estipular una remuneración a tanto alzado en determinados casos. En cualquier caso cuando se produzca una manifiesta desproporción entre la remuneración a tanto alzado y los beneficios obtenidos por el cesionario se deberá revisar el acuerdo fijando una nueva remuneración más equitativa.
- Respecto a lo no especificado en los contratos de cesión hay que tener en cuenta en la legislación sobre Propiedad Intelectual se establecen, salvo pacto explícito en contrario, las siguientes presunciones: la cesión no en exclusiva de las obras; la limitación temporal de los derechos cedidos a cinco años; la limitación del ámbito territorial autorizado para la explotación de las obras cedidas al del país en el que se realice la cesión; y la limitación de las modalidades de la explotación permitidas a los cesionarios a aquellas indispensables para cumplir la finalidad del contrato.

7. Protección de los derechos de autor

La protección de los derechos de autor se ve reforzada por diferentes medios entre los que cabe citar, por su especial relevancia, los siguientes:

- La protección registral, que actúa como presunción de veracidad de los derechos de autor inscritos en los Registros de la Propiedad Intelectual, desde el momento de su inscripción.
- La protección simbólica de las obras que incluyan el ã seguido del nombre del titular del derecho, y del lugar y año de divulgación de la obra, lo que indica que los derechos de explotación de la misma están reservados.
- La protección jurisdiccional ordinaria del Orden Civil, que permite utilizar las acciones generales de dicha jurisdicción para solicitar las oportunas indemnizaciones por los daños morales o patrimoniales causados por determinados actos que vulneran lo especificado en la legislación sobre Propiedad Intelectual; instar el cese de la actividad ilícita del infractor; y solicitar una especial protección de derechos de autor que incluya la intervención y deposito de los ingresos obtenidos por la actividad ilícita, el secuestro de los ejemplares y el embargo de los aparatos y materiales utilizados.

Asimismo y como medida preventiva se podrá solicitar a la autoridad judicial la adopción de las medidas cautelares que se considerasen necesarias para la protección de los derechos de los autores y titulares de los programas. Estas medidas, se tramitaran, caso de ser aceptadas, en forma preferente y en una forma tal que eviten eludir la acción de la justicia a los posibles infractores.
- La protección jurisdiccional del Orden Penal, que ante delitos relacionados contra la Propiedad Intelectual (reproducción, plagio, distribución, comunicación pública, transformación, importación, almacenaje o exportación de los programas sin autorización de los titulares o cesionarios de los mismos, y fabricación, puesta en circulación o tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger los programas) impone penas de prisión de seis meses a cuatro años, multas de seis a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido de dos a cinco años, autorizando al juez o tribunal a decretar el cierre temporal o definitivo de la industria o establecimiento del condenado.

7. Bibliografía

Alvarez Cienfuegos, José María; *Contratación informática: la protección penal de los programas de ordenador*. Encuentros sobre Informática y derecho 1994-1995. Editorial Aranzadi. Pamplona, 1996. Páginas 171 a 192.

Barriuso Ruiz, Carlos; *Interacción del Derecho y la Informática*. Editorial Dykinson. Madrid, 1996.

Bondía Román, Fernando; *Comentario a la ley 16/1993, de 23 de diciembre, de incorporación al derecho español de la Directiva sobre la protección jurídica de programas de ordenador*. Actualidad informática Aranzadi. Número 12. julio de 1994. Páginas 1 y 3 a 6.

Davara Rodríguez, Miguel Ángel; *Derecho informático*. Editorial Aranzadi. Pamplona, 1993.

Lamberterie, Isabel de; *Protección de programas de ordenador y relaciones contractuales*. Encuentros sobre Informática y derecho 1995-1996. Editorial Aranzadi. Pamplona, 1996. Páginas 27 a 36.

Orozco Pardo, Guillermo; *Informática y Propiedad intelectual*. Actualidad informática Aranzadi. Número 19. Abril de 1996. Páginas 1 a 5.

Pérez Luño, Antonio-Enrique; *Manual de informática y derecho*. Editorial Ariel. Barcelona, 1996.

Peso Navarro, Emilio del; *Protección jurídica: Programas de ordenador, bases de datos y multimedia*. Documentación del Seminario sobre "Software, bases de datos y multimedia. Su protección", organizado por IEE (Informáticos Europeos Expertos) y Granada: Computer Services International, impartido en Madrid el 2 de diciembre de 1997.

Peso Navarro, Emilio; Ramos González, Miguel Ángel; Fernández Sánchez, Carlos Manuel e Ignoto Azaustre, María José. *Manual de dictámenes y peritajes informáticos*. Análisis de casos prácticos. Editorial Díaz de Santos. Madrid, 1995.

LegisTIC

Retos jurídicos de Internet: el derecho a la intimidad

Javier Ribas
Dtor. del Departamento de Derecho de las Tecnologías de la Información de *PricewaterhouseCoopers*

<jribas@ibm.net>

A todos nos causaría extrañeza que al entrar en un comercio convencional, como una panadería, la cajera nos hiciese rellenar un formulario antes de comprar, nos pidiese una identificación plena y nos preguntase si el pan va a ser para consumo individual o familiar, para hacer un bocadillo o acompañar la comida, para consumir en casa o en la oficina. Mayor sería nuestro asombro si al salir de la panadería, el propietario del kiosco donde compramos el periódico nos hiciese rellenar otro formulario y nos dijese: "Veo que le gusta el pan integral, ¿conoce esta revista sobre dieta y salud?". Pero mucho más nos preocuparía que al llegar al portal de nuestra casa y mirar hacia la acera, viésemos que en el suelo han quedado las huellas de nuestros zapatos, mostrando todo el recorrido que hemos hecho, con nuestro nombre y dirección postal en cada una de ellas. Aunque ello resulta difícil de creer en un escenario presencial, es algo que puede llegar a suceder cuando vamos de compras por Internet. Existen una serie de dispositivos que permiten determinar nuestros hábitos de consumo y asociarlos a nuestra identidad digital. Ello no debería escandalizarnos puesto que si vivimos en un pueblo o en un barrio de una ciudad acostumbramos a renunciar a algunos aspectos de nuestra intimidad.

El panadero al que acudimos cada día sabe que el pan nos gusta un poco tostado, el señor del kiosco nos guarda los fascículos que le encargamos y nos recomienda un encuadernador y en el bar, al vernos entrar, el camarero se atreve a ponernos la cerveza y las aceitunas que pedimos normalmente.Pero la voluntariedad de esa pérdida de anonimato y de intimidad es la que puede marcar la diferencia entre ir de compras por la calle de una ciudad y hacer lo mismo en Internet. La posibilidad de que al visitar una página web se obtengan ciertos datos personales del usuario, sin su consentimiento, puede llegar a ser un obstáculo para la consolidación de la red como medio de comunicación, información y transacción comercial.

En la actualidad existe un sentimiento generalizado de que el usuario de Internet no es tan anónimo como se pretende y las últimas noticias sobre microprocesadores numerados y sistemas operativos chivatos no hacen más que alentar esa imagen orwelliana de Internet. La Agencia de Protección de Datos ya trabajó hace tiempo sobre esta cuestión y emitió unas recomendaciones para usuarios de Internet, que pueden ser consultadas en la dirección: *http://www.ag-protecciondatos.es.*

Cookies

Los *cookies* son pequeños ficheros de datos que se generan a través de las instrucciones que los servidores web envían a los programas navegadores y que se guardan en un directorio específico del ordenador del usuario.

El concepto y la finalidad del uso de *cookies* han cambiado con el tiempo, habiendo llegado a ser un poderoso instrumento de obtención de información para el administrador de un servidor y para los departamentos de marketing de empresas que hacen publicidad en Internet o simplemente disponen de una página web.

Esta técnica es objeto de debate en la actualidad, hasta el punto de que en Alemania existe un proyecto de ley que podría llegar a prohibir su uso.

Para determinar si se produce una intromisión en la intimidad del usuario, deben tenerse en cuenta una serie de cuestiones que se analizan a continuación.

Los *cookies* pueden contener datos personales o cualquier otro tipo de información relacionada con la interfaz cliente-servidor. La LORTAD define los datos personales como «cualquier información concerniente a personas físicas identificadas o identificables». Por ello, si el contenido está constituido por datos que son necesarios para efectuar transacciones cliente-servidor, en las que no se gestiona información relativa a personas físicas, no existirá una lesión potencial de la intimidad.

Algunos programas navegadores asignan de forma automática el nombre del usuario al fichero que se genera como *cookie*. De esta manera, el nombre del fichero puede estar formado por el nombre del usuario, un símbolo de separación y el nombre del servidor que ha dado instrucciones para generar el archivo *cookie*. Para que esta asignación pueda producirse, el navegador debe haber sido previamente personalizado por el usuario, en el momento de la instalación o con posterioridad.

Si ello no se produce, el contenido del *cookie* no podrá ser considerado como personal, ya que no podrá ser asociado a una persona identificada. No obstante, el archivo *cookie* puede contener la dirección IP del usuario. En este caso su identidad podría ser obtenida si utiliza una dirección IP fija, siempre que sea notorio el uso de dicha IP por un usuario determinado. En el caso de IP's dinámicas, la única forma de obtener la identidad del usuario sería mediante un requerimiento judicial al PSI que le dió acceso a la red, antes de que los datos de la sesión desaparezcan del *log* del sistema. Las dificultades inherentes a este sistema de identificación nos hacen pensar que la inclusión de una IP dinámica en un archivo *cookie* no es suficiente para considerar el contenido como datos de carácter personal.

También hay que tener en cuenta la finalidad que persigue el diseñador del *cookie* para poder valorar si su uso se ajusta o no a derecho. Por ejemplo, el administrador de una sede web puede ofrecer al usuario la posibilidad de personalizar la interfaz de usuario, es decir el menú, los contenidos y las diferentes opciones de diseño de la *home page* de un web. En este caso, la trascendencia del archivo *cookie* es mínima ya que responde a una finalidad pasiva de informar sobre la configuración de un navegador, o la *home page* de un servicio de noticias. En otros casos, la función del *cookie* es recoger datos sobre las secciones más visitadas de un web. Si todas las secciones tratan un tema monográfico, y la información es puramente estadística, tampoco vemos problemas. En especial, cuando la información estadística obtenida no puede asociarse a personas identificables. En cambio, cuando los datos obtenidos pueden servir para elaborar el perfil de un usuario concreto, y personalizar así la oferta posterior, pueden surgir conflictos con las disposiciones de la LORTAD, ya que la información se obtiene sin el consentimiento del usuario.

En este sentido, pueden ser declarados ilícitos los contenidos activos, es decir, aquéllos que no se limitan a ser un fichero de datos sino que pueden ser ejecutados de forma inconsentida, obteniendo mayor información. Nos referimos a programas que se instalan en el disco duro del ordenador y comprueban los datos personales que figuran en el ordenador del usuario, aprovechando la existencia de información (p.e. el historial de webs visitados) que pueden revelar sus gustos o preferencias.

Finalmente, debe analizarse el nivel de consentimiento del usuario, ya que el derecho a la intimidad es renunciable. Así, el usuario que mantenga una relación negocial con el propietario del servidor puede autorizarle contractualmente para que obtenga la información necesaria para concretar su oferta o para mejorar el servicio con prestaciones adicionales. En este caso, a la tradicional cláusula contractual por la que se autoriza el tratamiento automatizado de sus datos personales debe añadirse la figura del *cookie*, como instrumento para obtener datos adicionales sobre los hábitos de consumo, frecuencias de visita de una sección determinada, tipo de noticias a suministrar, etc. También puede obtenerse una autorización implícita mediante la advertencia de que la página web visitada tiene *cookies*, y que el usuario tiene la posibilidad de impedir el acceso a su ordenador, mediante la opción correspondiente de su navegador.

Lo que más molesta al usuario es la entrada de contenidos no consentidos en su ordenador. Si la página visitada tiene una sección que informa sobre las funciones que realiza el *cookie* y el usuario puede comprobar su carácter inofensivo, es probable que autorice su entrada en el sistema. En especial, si la recepción del *cookie* es un requisito previo para la visualización de la página, y ésta contiene algo que interesa al usuario.

Spam

Estados Unidos ha sido el país que más ha luchado contra la utilización del correo electrónico para el envío de publicidad no solicitada.

Además de las iniciativas legislativas para regular la publicidad a través de correo electrónico, destacan las demandas que se han producido contra los remitentes de mensajes publicitarios no solicitados.

Uno de los Estados que han prohibido el *spam* ha sido Washington. En junio de 1998 entró en vigor una ley que permite a cada destinatario de un mensaje publicitario no solicitado reclamar al remitente una compensación de 500 dólares.

En enero de 1998, la empresa Hotmail presentó una demanda (ver texto completo en *http://www.onnet.es*) contra ocho empresas que habían utilizado una dirección de este proveedor como remitente de una serie de mensajes comerciales no solicitados. Hotmail basaba su reclamación en un incumplimiento de las condiciones generales de contratación que los demandados habían aceptado on line, al contratar su cuenta de correo electrónico en Hotmail. Se trata de los contratos utilizados habitualmente en el comercio electrónico a través de Internet, basados en la presentación de un texto que incluye las condiciones en las que se va a prestar el servicio o se va a suministrar el producto, con un botón en el que aparece el texto "Aceptar", "OK" o "Estoy de acuerdo". Son los llamados *click-wrap agreements* o *point-and-click agreements*, ya que basan su validez en el acto de pulsar el botón de aceptación por parte del usuario y tienen gran similitud con las licencias *shrink-wrap* utilizadas en la comercialización de software empaquetado, que se aceptan mediante el desprecintado y la apertura del sobre o envoltorio que contiene los soportes físicos donde va el programa.

La dificultad de este tipo de acuerdos estriba en que no existe una firma o una muestra de consentimiento que se conserve como prueba de la aceptación del usuario. No obstante, la mayoría de las transacciones electrónicas que se realizan en la actualidad se basan en acuerdos que se aceptan pulsando un botón de una página web, por lo que, con el tiempo, deberá aceptarse esta forma de aceptación, cuando se cumplan los requisitos necesarios para ello.

En mayo de 1998, el tribunal californiano entendió que había suficiente base documental para apreciar la validez del contrato y aceptó las medidas cautelares solicitadas por Hotmail.

Otros casos que demuestran el rechazo del *spamming* por los usuarios de Internet son los siguientes:
- En enero de 1997, un abogado de Tennessee fue expulsado del Colegio de Abogados por enviar mensajes publicitarios a más de cinco mil grupos de noticias y a miles de direcciones de correo electrónico.
- En febrero de 1997, **Compuserve** consiguió que se dictaran medidas cautelares contra la empresa **Cyber Promotions**, que consistían en la prohibición de enviar mensajes publicitarios no solicitados a los usuarios de Compuserve.

- En octubre de 1998, **America Online (AOL)** consiguió una medida cautelar contra la empresa **IMS** por haber enviado más de 60 millones de mensaje a los suscriptores de AOL.

- En diciembre de 1998 America Online (AOL) presentó nueve demandas contra presuntos *spammers* que dirigían mensajes no solicitados a sus usuarios y consiguió una medida cautelar de prohibición de envío de mensajes contra otra empresa.

En Europa, la propuesta de Directiva sobre comercio electrónico (ver texto completo en *http://www.onnet.es*) dispone de una sección dedicada a la publicidad no solicitada y la Directiva sobre contratos a distancia sólo establece restricciones a la utilización de sistemas automatizados de llamada sin intervención humana (llamadas automáticas) y del fax, sin el consentimiento previo del consumidor, aunque a continuación añade que los Estados miembros velarán por que las técnicas de comunicación a distancia distintas de las antes mencionadas, cuando permitan una comunicación individual, sólo puedan utilizarse a falta de oposición manifiesta del consumidor.

En España, la Agencia de Protección de Datos ha redactado una guía para usuarios de Internet que puede obtenerse gratuitamente en *http://www.ag-protecciondatos.es*

Informe de la FTC sobre marketing e intimidad en Internet

La **Federal Trade Commission** norteamericana (**FTC**) ha publicado un informe sobre "Intimidad *on line*" en el que se describe cómo se obtienen los datos personales de los usuarios que visitan los webs comerciales de las empresas americanas y se analiza la política de las mismas respecto a la información al usuario sobre la recogida de dichos datos.

El informe de la FTC ofrece las siguientes conclusiones:
Webs comerciales visitados que obtienen información relativa a personas identificables: 90%
Webs comerciales visitados que informan al usuario sobre dicha obtención de datos. 14%
Webs comerciales visitados que informan al usuario sobre su política en materia de intimidad: 2%
Webs destinados al público infantil que obtienen información personal de los visitantes: 89%
Webs destinados al público infantil que informan sobre dicha obtención de datos: 54%

Al final del informe, la FTC recomienda al Congreso que regule la forma en que las empresas obtienen información personal a través de sus sedes web en Internet, especialmente, respecto al público menor de 13 años.

Caso Geocities

Geocities, uno de los más populares proveedores de Internet que ofrecen albergue gratuito de páginas web, ha llegado a un acuerdo por el que se pone fin al procedimiento iniciado por la **Federal Trade Commission (FTC)**, en el que lo acusaba de utilizar los datos personales de sus usuarios con una finalidad distinta a la indicada inicialmente.

En el acuerdo, Geocities se obliga a publicar en su página web un aviso sobre intimidad, explicando a los usuarios qué información está siendo obtenida de los mismos y con qué propósito, a quién será transmitida y cómo pueden los afectados acceder a dichos datos y exigir su cancelación.

Además, Geocities deberá conseguir el consentimiento paterno antes de obtener información de usuarios menores de 13 años.

La comunidad virtual de Geocities tiene más de dos millones de miembros, divididos en diversos barrios temáticos, donde los usuarios albergan sus páginas web con contenidos comunes de forma gratuita. Cuando un usuario quiere convertirse en miembro de Geocities, debe completar un formulario en el que se solicita información personal. En el momento de la investigación realizada por la FTC, algunos de los datos solicitados eran obligatorios y otros eran opcionales. El formulario también pregunta al usuario si desea recibir ofertas especiales para miembros de Geocities, por parte de otros anunciantes.

Mediante este procedimiento de registro, Geocities introducía la información obtenida en una base de datos que incluía:
- direcciones postales
- direcciones de correo electrónico
- áreas de interés del usuario
- ingresos
- formación
- sexo
- estado civil
- ocupación

Según la FTC, esta información permitía generar perfiles de usuarios y ceder ficheros de datos segmentados a diversos anunciantes. Ello implicaba una disposición no autorizada de los datos, ya que los afectados facilitaban dicha información conscientes de que el contenido de los campos obligatorios podía ser utilizado para remitir ofertas específicas que ellos solicitaban, y que el contenido de los campos opcionales no sería cedido a terceros.

Autorregulación

En este momento en el que factores como el aumento de las tarifas telefónicas o el mal funcionamiento de ciertos sistemas de acceso han ralentizado el crecimiento del número de usuarios de Internet en nuestro país, lo último que debemos hacer es promover la creación de nuevas barreras que impidan la popularización de la red. Creo que tanto la oferta como la demanda están de acuerdo en que hay que eliminar los obstáculos y los factores inhibidores que impiden la consolidación del comercio electrónico como nuevo motor de la economía que contribuya a un mayor bienestar social y a la creación de puestos de trabajo.

Por ello, al tiempo que proliferan los sistemas de navegación anónima y se implantan los micropagos anónimos, se debe trabajar en la autorregulación. Y en este sentido debe aplaudirse la iniciativa de la **Asociación Española de Comercio Electrónico** (*http://www.aece.org*), al publicar un código dirigido justamente al tratamiento de los datos personales que se obtienen a través de Internet. La adhesión a este código por parte de un comercio que opere en la red le permite utilizar un sello de calidad en su página web, de manera que los usuarios que la visitan pueden tener la confianza de que su derecho a la intimidad será respetado. El cliente puede acceder, en la página principal, a un documento en el que el comercio le informa sobre el uso que va a hacer de los datos personales que facilite y dispone de medios eficaces para rectificar o cancelar dichos datos.

La protección del anonimato y de la intimidad en Internet serán objeto de debate durante los próximos años, pero sólo un compromiso entre los objetivos del *marketing* y la confianza del usuario nos ayudará a conseguir la red que todos queremos.

LegisTIC

Miguel Ángel Davara Fernández de Marcos
Profesor de ICADE. Universidad Pontificia Comillas

Los nombres de dominio y los derechos de propiedad intelectual

1. Introducción

El gran desarrollo que se ha producido en Internet en los últimos años y las perspectivas de que este desarrollo sea cada vez mayor han puesto de relevancia la importancia de los nombres de dominio, teniendo su más importante reflejo en el aspecto comercial[1]. Es en este campo donde mayor número de controversias se pueden plantear, por las prácticas fraudulentas que se pueden realizar con los nombres de dominio[2].

Si bien los nombres de dominio fueron ideados con objeto de identificar ordenadores, su principal importancia la han adquirido como identificadores comerciales. Así, han provocado graves conflictos con la protección, mediante los derechos de propiedad intelectual, de los identificadores comerciales.

Debido a los comienzos de Internet, que se sitúan en Estados Unidos, es en este país donde radica la entidad encargada de proporcionar los nombres de dominio. Sin embargo, tras haber finalizado el plazo de concesión de esta facultad, ahora se plantea la posibilidad de realizar un cambio que permita, entre otras cosas, su universalización, de manera que no pertenezca solamente al ámbito estadounidense.

2. Una primera aproximación

Los nombres de dominio los podríamos clasificar en dos categorías: los nombres de dominio de primer nivel (*Top Level Domain*, o **TLD**) y los nombres de dominio de segundo nivel (*Second Level Domain*, o **SLD**).

Los de primer nivel se dividen, a su vez, en otras dos categorías, puesto que existen unas categorías genéricas (.com, .edu, .org, .net., ...) y otras que podríamos denominar territoriales, o *country-code*[3] (normalmente serán los dos primeros caracteres del nombre de cada país)[4].

Respecto a los nombres de dominio de primer nivel (los genéricos normalmente son citados como **gTLD**) su principal problema radica en los supuestos en los que dos personas (físicas o jurídicas) registran un nombre de dominio de segundo nivel con dos nombres de dominio de primer nivel distinto (normalmente un nombre de dominio genérico, y otro territorial)[5].

Además, la importancia de estos nombres de dominio de primer nivel puede radicar también en su utilización por parte de empresas que entiendan que el nombre completo puede ser aún más fácil de recordar por los usuarios[6].

Los nombres de dominio de segundo nivel se corresponden con el que precede al de primer nivel, esto es, con lo que normalmente será identificado por el usuario para conocer el sitio en el que se encuentra. La asignación de estos dominios corresponde a la entidad que tenga atribuido el nombre de primer nivel bajo el que se registra.

En España, el registro de estos nombres constituye, como señala Maestre[7], un servicio público, que se presta por el Centro de Comunicaciones **CSIC**, **RedIRIS**, integrado en el Consejo Superior de Investigaciones Científicas (CSIC), y que se denomina **ES-NIC**.

Respecto a estos nombres de dominio de segundo nivel, los problemas que nos podemos encontrar son muy variados.

Según Mueller[8], los actuaciones respecto a los nombres de dominio de segundo nivel, en su relación con las marcas, los podemos dividir en cuatro categorías:
Infringement, que comprendería los conflictos en los que el titular del nombre de dominio actuaba con intención de utilizar en su beneficio la reputación de otra marca.

Speculation, realizada cuando se registra un nombre de dominio coincidente con otra marca, que no va a ser utilizado, con el único objeto de que la marca en cuestión se vea obligada a "recomprarlo"[9].

String conflicts, considerando dentro de esta categoría los casos en los que más de una persona tiene, aparentemente, derecho a utilizar un mismo nombre.

Parody, preemption and other, que la considera una categoría residual donde incluir los casos que no encajan en ninguna de las categorías anteriores.

3. Propiedad intelectual

De acuerdo con el Informe de la **Organización Mundial de la Propiedad Intelectual**[10] (**OMPI**)[11] entendemos que el conflicto de la gestión y distribución de nombres de dominio con los derechos de propiedad intelectual es uno de los principales problemas que podemos encontrar. Según este mismo informe, podríamos clasificar los principales motivos de protección de los derechos de propiedad intelectual en dos: el primero sería el de proteger las creaciones intelectuales, con objeto de posibilitar su profusión, y el segundo sería el de permitir el correcto funcionamiento del mercado basado en estas creaciones intelectuales.

El primer motivo, referido a la protección de las propiedades

intelectuales con objeto de incitar nuevas creaciones se llevaría a cabo permitiendo la obtención de una recompensa por la obra original, y por la inversión realizada. Por otra parte el correcto funcionamiento del mercado se refiere a la intención de evitar la confusión de los consumidores respecto al origen de unos productos asociados a un determinado nombre o marca.

Si consideramos que el sector cuaternario, o del conocimiento, es hoy en día un sector básico en la economía mundial, y que muchas fuentes de riqueza están basadas en aspectos intelectuales, comprenderemos la importancia de la protección de los derechos de propiedad intelectual.

Como hemos señalado anteriormente, una parte de los nombres de dominio se registran con objeto de obtener un lucro mediante operaciones posteriores con las empresas que tengan el nombre registrado.

Esta práctica puede entrar en conflicto con los derechos de propiedad intelectual que se tratan de proteger por otras vías. Así, la OMPI ha tratado de realizar una proceso de interfaz entre el sistema de nombres de dominio y la propiedad intelectual (o más específicamente las marcas).

Los problemas entre ambas se han visto agravados por la cantidad de "prácticas predatorias y parasítarias adoptadas por algunos para explotar la falta de conexión entre los fines para los que se diseñó el DNS[12] y aquellos para los que existe la propiedad intelectual. Estas prácticas incluyen el registro deliberado y de mala fe, como nombres de dominio, de marcas notoriamente conocidas y otras con la esperanza de poder vender los nombres de dominio a los titulares de dichas marcas o simplemente de tener una ventaja deshonesta sobre la reputación de dichas marcas".[13]

Respecto a los conflictos que han surgido por estas prácticas, encontramos cada vez más casos ante los tribunales. Así, si ya hemos comentado el problema suscitado en España con el buscador Ozú, podemos mencionar como uno de los casos más claros el *One in a Million LTD*, en Inglaterra[14]

El problema de la notoriedad de las marcas famosas es asimismo abordado por el Informe de la OMPI, señalando que la protección de las mismas viene reconocida por el **Convenio de París** para la propiedad Industrial, y el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio.

Después de analizar los problemas que se pueden contemplar respecto a la aplicación de estas normas al espacio cibernético, propone tres mecanismos de solución:
"i) un mecanismo para obtener y aplicar la exclusión de la utilización de una marca famosa y notoriamente conocida en un TLD abierto;

ii) un recurso probatorio para garantizar que la protección concedida por una exclusión puede ser ampliada a registros de nombres de dominio idénticos o similares, susceptibles de inducir a error;

iii) el reconocimiento del registro abusivo de un nombre de dominio como base para la anulación o transferencia de dicho registro".

Los principales problemas con los que se han encontrado los titulares de derechos de propiedad intelectual, especialmente aquellos titulares de marcas famosas, no son los de la confluencia de dos derechos aparentemente legítimos sino aquellos de abuso flagrante.

Algunas empresas han llevado a cabo unas prácticas defensivas cuyo resultado no podrá ser otro, en caso de que se realice de manera indiscriminada, que el bloqueo, por uso abusivo, de las direcciones de Internet[15].

Aunque las medidas que se proponen para tratar de solucionar los conflictos se llevasen a cabo, el problema que surge inmediatamente es el de su aplicabilidad por parte de los Estados. No debemos olvidar la universalidad de Internet, y sus consiguientes dificultades de regulación[16].

Además, debemos añadir a esto la diferencia existente entre el poco gasto que supone el registro de un nombre de dominio, y el alto coste que se puede causar a una empresa por su utilización fraudulenta, e igualmente, el alto coste, y el tiempo que se necesita para recuperar (adquirir) un nombre de dominio por la vía judicial[17], es por lo que las medidas reseñadas son ejecutables a *priori*. Para evitar este problema, la OMPI propone que las partes se acojan a un sistema de arbitraje, pero éste es un sistema voluntario.

4. Conclusión

Los nombres de dominio han adquirido una gran importancia debido al desarrollo de Internet, lo cual ha provocado la existencia de un número cada vez mayor de conflictos con otros derechos, entre los cuales destaca el derecho de propiedad intelectual.

Los problemas con estos derechos no se han producido tanto por confluencia de dos personas con derechos aparentemente legítimos, cuanto por las prácticas fraudulentas que se han llevado a cabo. Especialmente con las marcas famosas, se ha producido el hecho de personas que han registrado sus nombres con el único objeto de revenderlo por un precio mayor.

A la hora de recuperar los derechos sobre un nombre de dominio, se produce un desequilibrio entre lo económico que resulta obtener el nombre y lo costoso que resulta, por parte de la empresa titular de los derechos de propiedad intelectual, recuperarlos judicialmente.

Las posibles soluciones que se han planteado para este problema serían, una de carácter preventivo que consistiría en intentar bloquear las peticiones de personas ajenas a las empresas conocidas de los nombres de dominio que coincidieran con las denominaciones de estas empresas, y otro a posteriori, que consistiría en desarrollar un sistema de solución de conflictos (que podría ser un arbitraje) que fuese más rápido y económico, pero su mayor dificultad reside en la necesidad de que las partes deseen someterse a él.

Notas

[1] Todas las empresas (o particulares) que deseen ofertar productos a través de Internet o que, en general, quieran obtener algún beneficio material de su inclusión en la red, deben tener una dirección (un nombre de dominio) que sea fácil de recordar por aquellas personas que accedan a su página alguna vez.
[2] Aun en las situaciones en que la problemática planteada se refiera a los

derechos de propiedad intelectual, el trasfondo que tiene es, en una gran cantidad de casos, económico.

[3] A veces se citan como ccTLD (*Country-code Top Level Domain*)

[4] En España es el nombre de dominio ".es".

[5] En este sentido, en España tenemos el caso del buscador "Ozu", en el que, mientras una entidad registró el nombre "Ozu.es", otra persona registró en Estados Unidos el nombre "Ozu.com"

[6] Un ejemplo clarísimo en este sentido lo hemos tenido hace unos meses, cuando una empresa ha comprado por una cantidad muy alta de dinero los derechos para poder otorgar los nombres de dominio de las Islas Tuvaru. El motivo de tal compra es que el dominio otorgado a este país es .tv, y la empresa compradora estimó que las empresas de televisión de cualquier lugar del planeta preferirán que su dirección de Internet finalice de esta manera, para evitar así problemas a la hora de recordarla, puesto que a veces se duda sobre si la dirección a la que queremos acudir tiene un nombre de dominio de primer nivel genérico (por ejemplo, .com) o territorial (por ejemplo .es)

[7] **Maestre Rodríguez, Javier A.**, "Planteamiento de la problemática jurídica de los nombres de dominio", en la *Revista Actualidad Informática Aranzadi*, núm. 29, ed. Aranzadi, Pamplona, octubre de 1998.

[8] **Mueller, Milton** establece una clasificación, según refleja el Boletín de los Nombres de Dominio, núm. 6, de 1 de julio de 1998, actualmente localizable en la dirección de Internet *www.dominiuris.com/boletines*, respecto a los nombres de dominio de segundo nivel, en relación a las marcas.

[9] Ya hemos explicado la importancia que, para una entidad determinada puede tener el hecho de que sus clientes (o potenciales clientes) sean capaces de identificarla en la red sin problemas.

[10] Estos comentarios están disponibles en la dirección de Internet de dicha organización, que es *wipo2.wipo.int*

[11] Las siglas de OMPI en inglés, más extendidas, son WIPO.

[12] DNS (*Domain Name System*), o Sistema de Nombres de Dominio.

[13] El mismo informe señala en otro punto que " En el mundo comercial, la fama con frecuencia se manifiesta en reputación y con frecuencia la reputación se adjunta como expresión de la identidad de la empresa: sus marcas. Las marcas famosas y notoriamente conocidas han sido el blanco especial de varias prácticas predatorias y parasítarias en Internet. Se han creado varias palabras para describir estas prácticas: "ocupación ilegal del espacio cibernético" (en inglés *cibersquatting*), cuando una persona registra como nombre de dominio una marca, con frecuencia famosa y notoriamente conocida que pertenece a un tercero, aprovechando la práctica de registro de atender en orden de presentación, con la esperanza de bloquear al propietario de la marca en su utilización como nombre de dominio o de poder vender el registro del nombre de dominio al titular, a cambio de una prima considerable que de cualquier manera sería menor a la cantidad que el titular debería pagar si entablara un litigio para deshacerse del ocupante ilegal del espacio cibernético; y la "acumulación" (*warehousing*), cuando una persona registra muchas de esas marcas como nombres de dominio y acumula así una colección digital de marcas que puede ofrecer en venta."

[14] En este caso, las empresas British Telecommunications Plc, Virgin Enterprises Ltd, J Sainsbury Plc, Marks & Spencer Plc, Ladbroke Group Plc, actuaron contra la entidad One In A Million Ltd porque esta entidad se dedicaba a registrar nombres de dominio de compañías famosas, para posteriormente revenderlos. Se puede encontrar la Sentencia de la *Supreme Court Of Judicature* en la dirección *http://www.nic.uk/news/oiam-appeal-judgment.html*

[15] Así, ha habido empresas que, observando que otras personas registraban su nombre de dominio con un TLD distinto, han optado por acudir a muchos países a registrar su nombre, así como con todos los gTLD existentes, aunque el contenido de la página sea el mismo.

[16] Debido a que Internet no tiene una única sede jurisdiccional y que cada Estado tiene sus propias normas (incluso las normas más comúnmente aceptadas no lo son por todos los Estados), la dificultad de aplicabilidad de las normas dictadas es mayor.

[17] Esto provoca que muchas veces los conflictos los diriman las partes mediante acuerdos extrajudiciales, en los que normalmente se sitúa con más fuerza la parte poseedora del dominio.

LegisTIC

Breves consideraciones sobre determinados aspectos jurídicos del comercio electrónico en el mercado interior*

Isabel Hernando
Profesora Titular de la Facultad de Derecho San Sebastián, Dtra. General Fundación ISLT (Instituto para la Seguridad Legal y Técnica de las Tecnologías de la Información y de las Comunicaciones)

* Este artículo se inscribe dentro del proyecto CICYT "Productos Multimedia y servicios *on-line*: Seguridad Jurídica", dirigido por la autora

0.Introducción

El Comercio Electrónico ofrece a la Comunidad una oportunidad única de incrementar la competitividad de la industria europea, de promover el desarrollo económico y de impulsar las inversiones innovadoras y la generación de puestos de trabajo. Ahora bien, este máximo rendimiento del comercio electrónico sólo es posible obtener si se procede a la supresión de los numerosos impedimentos jurídicos que persisten en el sector de la prestación de servicios en línea.

Mediante la propuesta de Directiva de 18 de enero de 1998 [1] se pretende eliminar dichos obstáculos. La Propuesta de Directiva se aplica a los "servicios de la sociedad de la información", es decir, *a todo servicio prestado, normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario del mismo.*[2] Esta definición comprende una enorme variedad de áreas y actividades que se pueden realizar en línea, por ejemplo, periódicos electrónicos, enciclopedias en línea, servicios de venta de determinados productos como automóviles, servicios educativos, servicios profesionales (médicos, abogados, expertos contables), servicios turísticos, servicios de agencia inmobiliaria, servicios de anuncios breves, supermercados virtuales, servicios de agencia inmobiliaria, tablones de anuncios electrónicos, motores de búsqueda, servicios de acceso a la WWW, servicios de videojuegos, foros de discusión, servicios de ocio, etc…

El objetivo principal de la presente propuesta de Directiva es el de garantizar el correcto funcionamiento del mercado interior de forma que los servicios de la sociedad de la información puedan beneficiarse plenamente de la libre prestación de servicios entre los Estados miembros. La actual propuesta complementa el ordenamiento jurídico comunitario aplicable a tales servicios y se mantiene el actual nivel de protección del consumidor y de la salud pública, establecidos por los instrumentos comunitarios. En la propuesta se analizan cinco cuestiones esenciales que forman un conjunto coherente y que afectan al régimen del mercado interior: el establecimiento de los prestadores de servicios, las comunicaciones comerciales, los contratos por vía electrónica, la responsabilidad de los intermediarios, la aplicación de normativas.

1. Lugar de establecimiento de los prestadores de servicios de la Sociedad de la Información

Como aspecto esencial para el correcto funcionamiento del mercado interior, la propuesta pretende la eliminación de la inseguridad jurídica que existe en este ámbito al determinar el lugar de establecimiento de los prestadores de servicios de la sociedad de la información, de conformidad con los principios enunciados en el Tratado y la jurisprudencia del Tribunal de Justicia.

A este fin, responden los criterios estipulados en la propuesta de Directiva: la prohibición de regímenes de autorización para los servicios de la información y los requisitos que, con respecto a la información, el prestador de servicios deberá cumplir para garantizar la transparencia de sus actividades.

(1) La prohibición de regímenes de autorización para los servicios de la información. El objetivo de esta prohibición (art. 4) es el de la aplicación del principio de libertad de establecimiento, posibilitando el acceso a las actividades de prestación de servicios en Internet. El artículo 4 que, contiene el principio de no autorización previa, pretende propiciar, según términos de la propuesta el establecimiento de un especie de "derecho de sitio" que pertenecerá a cualquier empresa, operador o trabajador autónomo que decida prestar un servicio vía Internet.

No obstante, esta prohibición no "*irá en perjuicio de los regímenes de autorización que no tienen por objeto específico y exclusivo los servicios de la sociedad de la información o de los regímenes de autorización que estén cubiertos por la Directiva 97/13/CE*" de 15 de diciembre de 1997[3]

(2) Los requisitos que, con respecto a la información, el prestador de servicios deberá cumplir para garantizar la transparencia de sus actividades. Bajo este epígrafe, la propuesta de Directiva fija los datos concernientes al prestador de servicios a los que las autoridades competentes así como los destinatarios de los servicios pueden acceder con independencia de la existencia de una posible relación contractual: [4]

(a) nombre del prestador de servicios
(b) dirección en que está establecido el prestador de servicios
(3) datos que permitan ponerse en contacto rápidamente con el prestador de servicios y establecer una comunicación directa y efectiva con él, incluyendo su dirección de correo electrónico
(4) si el prestador de servicios está inscrito en un registro mercantil, nombre de dicho registro y número de inscripción asignado en él al prestador de servicios.
(5) Si una determinada actividad está sujeta a un régimen de autorización, las actividades cubiertas por la autoridad concedida al prestador de servicios y los datos de la autoridad que la haya concedido.

(6) Por lo que se refiere a las profesiones reguladas:
- si el prestador de servicios pertenece a un colegio profesional o institución similar, datos de dichos colegio o institución.
- título profesional expedido en el Estado miembro en que esté establecido, normas profesionales aplicables en el Estado miembro en que esté establecido y en los Estados miembros en que se suministran de forma regular servicios de la sociedad de la información.
(7) si el prestador de servicios ejerce una actividad gravada por el IVA, el número de iVA con el que está registrado en la administración de hacienda que le corresponda.

Esta información debe ser proporcionada de forma directa, permanente y fácilmente accesible. Por último, dentro de esta obligación de información, la propuesta de Directiva delega a las leyes de los Estados miembros la regulación de los precios de los servicios de la información que deberán constar de forma precisa e inequívoca.

2. Comunicaciones comerciales (publicidad, *marketing* directo, etc.)

Otro aspecto fundamental de los servicios de comercio electrónico está constituido por las comunicaciones comerciales. Con el fin de facilitar y precisar su utilización la propuesta de Directiva procede a estipular los siguientes aspectos:
(1) La definición del concepto de "comunicaciones comerciales" y la fijación con respecto a ellas de los requisitos de transparencia necesarias para fomentar las prácticas comerciales leales y la confianza de los consumidores.
(2) Las prácticas de *spamming*
(3) Las comunicaciones comerciales de las prácticas reguladas

(1) La definición del concepto de "comunicaciones comerciales" y la fijación de requisitos. Las comunicaciones comerciales, según la Directiva, deberán respetar las siguientes obligaciones:
(a) La obligación de identificación clara de la condición de comunicación comercial (por ejemplo, los rótulos comerciales mediante iconos o imágenes).
(b) La obligación de identificación clara de las personas físicas o jurídicas en nombre de las que se hace la comunicación comercial.
(c) La obligación de transparencia en el caso de las ofertas de promoción (descuentos, primas, regalos) y de las condiciones para beneficiarse de ellas.
(d) La obligación de transparencia para los concursos y juegos de promoción que tienen un objetivo de comunicación comercial y para las condiciones de participación.

(2) Las prácticas de spamming. En la propuesta se trata de la comunicación comercial no solicitada disponiendo que, con el fin de que los consumidores puedan reaccionar con mayor rapidez en caso de injerencia perjudicial, las comunicaciones comerciales realizadas por correo electrónico deberán ser claramente identificables en el momento mismo en que el destinatario las reciba.

A este respecto, la propuesta no aporta mayores precisiones y sirve de complemento a la Directiva 97/7/CE (art. 10) [5] y a la Directiva 97/66/CE del Parlamento Europeo y del Consejo referente a los datos de carácter personal y a la protección de la intimidad en el sector de las telecomunicaciones. [6] El artículo 12 (2) de esta última dispone, a este efecto, que las comunicaciones no solicitadas por correo electrónico deben recibir una marca especial en el sobre para que el destinatario de este tipo de mensajes pueda darse cuenta de forma inmediata de que se trata de una comunicación comercial sin tener que proceder a su apertura.

(3) Las comunicaciones comerciales de las prácticas reguladas. Con respecto a las profesiones reguladas (como la abogacía), la propuesta de Directiva estipula el principio general de autorización de la comunicación de modo que las legislaciones nacionales relativas a la comunicación comercial permitan la prestación de servicios en línea siempre que se respeten las normas de deontología sobre publicidad, independencia, dignidad y honor de la profesión, secreto profesional y lealtad hacia clientes y colegas.

Con este fin, se exhorta a las organizaciones profesionales a elaborar códigos de conducta en los que los organismos responsables examinen en especial dos tipos de información: la *indicación de las especialidades y de las tarifas*, fundamentales, ambas, para la protección del consumidor y para la actividad económica.

3. Celebración de contratos en línea

La celebración de contratos en línea es uno de los pilares fundamentales del desarrollo del comercio electrónico. A este fin, la propuesta de Directiva tiende a eliminar la inseguridad jurídica instando a los Estados miembros a revisar sus leyes. proponiendo las siguientes pautas:
(1) Régimen jurídico
(2) Modalidades de formación de contratos
(3) Momento de celebración del contrato

(1) Régimen jurídico. Los Estados miembros están sujetos, según la propuesta de Directiva, a una obligación de resultados. Esta obligación consiste en realizar un *examen sistemático de las normativas* que pueden entorpecer la *utilización real* de los contratos por vía electrónica.

Este examen contempla el conjunto de las etapas del proceso contractual que incluyen, por ejemplo: la oferta de contrato, la invitación a efectuar una oferta de contrato, la negociación, la celebración contractual, la modificación o resolución del contrato, la facturación y archivo del contrato. Transponiendo esta obligación, los aspectos a tener en consideración por los Estados miembros son, entre otros, los siguientes:
- La supresión de las disposiciones que conduzcan a privar de efecto y validez la utilización de las vías electrónicas.
- La adaptación de los requisitos formales que no puedan ser realizados por vía electrónica. Como ejemplo aparecen los siguientes:
· Requisitos referentes al soporte físico del proceso contractual (papel, número de originales, contrato publicado o impreso).
· Requisitos concernientes a la presencia humana: negociarse o celebrarse con personas físicas o en presencia de ambas partes o en lugares concretos.
· Requisitos en relación a la participación de terceros: autenticarse ante notario, celebrarse en presencia de terceros, depositarse o registrarse.

- La adaptación de forma armonizada de las condiciones fiscales.

Por último, la propuesta prevé un régimen de excepciones en las que puede ser legítimo restringir el uso de los contratos *on-line* a la vez que solicita a los Estados miembros que comuniquen los contratos que pueden acogerse a esta excepción.

Entre los contratos exceptuados por la propuesta de Directiva figuran los siguientes: *"Contratos que requieran la intervención de un notario", "Contratos que, para ser válidos, deban registrarse ante una autoridad pública", "Contratos sujetos al derecho de familia"* y *"Contratos sujetos al derecho de sucesiones"*.

(2) Modalidades de formación de contratos. Las modalidades de formación de un contrato por vía electrónica, según la propuesta de la Directiva, deberán estar supeditadas al principio de transparencia. Esta obligación que afecta al prestador de servicios comprende, entre otras, las siguientes actividades de información:
- Una descripción anticipada de las diversas operaciones necesarias para realizar formalmente el contrato.
- La posibilidad de proporcionar al destinatario del servicio, salvo acuerdo en contrario de las partes y siempre que se trate de profesionales, los códigos de conducta que puedan existir sobre los aspectos contractuales que debe respetar el prestador así como los datos que permitan acceder a dichos códigos vía electrónica.

(3) Momento de celebración del contrato. La propuesta de Directiva analiza un tipo de situación que presenta una enorme inseguridad jurídica en cuanto a la determinación del momento de celebración del contrato:
- Se trata de un proceso contractual en el que el destinatario del servicio sólo puede elegir entre hacer *click* en los iconos para rechazar o aceptar una oferta y
- Se trata de una oferta formulada por un prestador de servicios.

Ante esta situación, los principios que se proponen para considerar celebrado el contrato son las siguientes:
(a) Se precisa que el destinatario del servicio *"haya recibido por vía electrónica una notificación del prestador de servicios acusando recibo de la aceptación del destinatario del servicio y haya confirmado la recepción del acuse de recibo"*.
(b) Se entenderá recibido el acuse de recibo y realizada la confirmación "*cuando las partes a las que van destinados puedan tener acceso a los mismos"*.
(c) Ambos, el acuse de recibo y la confirmación "*deberán enviarse lo antes posible"*

Siguiendo con su objetivo de mantener la transparencia en las operaciones y la lealtad entre las partes, la propuesta encomienda a las autoridades nacionales que exijan al prestador de servicios la puesta a disposición de los destinatarios del servicio de los medios adecuados para permitirle conocer sus errores de manipulación y corregirlos. .

4. Responsabilidad de los intermediarios

Bajo este epígrafe se pretenden fijar los límites en materia de responsabilidad que incurren los prestadores de servicios en línea cuando actúan como "intermediarios" mediante la transmisión y almacenamiento de datos potencialmente ilícitos pertenecientes a terceras personas (por ejemplo, derechos de autor pirateados, competencia desleal, publicidad engañosa).

En la propuesta, la clasificación referente a la responsabilidad se basa en el tipo de actividad ejercida [mero transporte (1), *caching* (2), alojamiento (3)], y no en el tipo de operador. Estas actividades se caracterizan, por otra parte, por los siguientes aspectos: los destinatarios del servicio son los que ofrecen la información, la información se almacena o transmite a petición de los destinatarios del servicio, el destinatario es la persona que ofrece información en línea y la que tienen acceso a la misma o la recupera. La pretensión de la propuesta de Directiva es la de conseguir "*un equilibrio prudente entre los distintos intereses que están en juego, de forma que se fomente la cooperación entre las partes y, de esta manera, se limite el riesgo de que haya actividades ilícitas en línea".*[7]

(1) Mero transporte (*mere conduit*). El artículo 12 de la propuesta estipula una exención de responsabilidad para las actividades de transmisión en red de datos suministrados por el destinatario del servicio o de concesión de un acceso a la red de comunicaciones. De conformidad con esta exención, el prestador de servicios desempeña un papel pasivo y no se podrá proceder a la reclamación por daños y perjuicios con independencia del tipo de responsabilidad civil o penal de que se trate. La exención, según el precepto, no excluye la posibilidad de una acción de cesación.

No obstante, para que pueda aplicarse la exención, es necesario que se cumplan las siguientes condiciones:
· Que el prestador de servicios *no transmita su propia información*. En caso contrario, no podrá ser considerado como intermediario.
· Que el prestador de servicios *no haya originado la transmisión.* En este supuesto, el prestador de servicios no debe adoptar la decisión de efectuar la transmisión. Esta condición se cumple cuando, según los términos de la propuesta, el prestador procede automáticamente a una transmisión a petición de un destinatario del servicio.
· Que el prestador de servicios *no seleccione ni modifique* los datos transmitidos.

Por último, la propuesta contempla dentro de la exención, la actividad de "mero transporte" que se refiere al almacenamiento provisional y transitorio que sucede durante la transmisión de la información y cuyo único objetivo sea permitir la ejecución de la misma. La duración de este almacenamiento no debe superar el tiempo razonablemente necesario para la transmisión.

(2) *Caching.* La propuesta contempla, a continuación, en su artículo 13, la forma de almacenamiento temporal de la información denominada *system caching*. Este sistema de almacenamiento permite aumentar el rendimiento y rapidez de las redes digitales sin que suponga un aprovechamiento separado de la información transmitida.

El proveedor de los servicios está exonerado, según la propuesta, de toda responsabilidad derivada de este tipo de almacena-

miento siempre que respete las condiciones siguientes:
- Que no exista una modificación de la información por parte del prestador del servicio.
- Que se respeten las condiciones de acceso a la información por parte del prestador del servicio
- Que "*el prestador del servicio respete las normas relativas a actualización de la información, indicadas de forma coherente con las normas del sector"*.
- Que "*el prestador del servicio no interfiera en la tecnología coherente con las normas del sector que se utilice con el fin de obtener datos sobre utilización de la información"*
- Que "*el prestador del servicio actúe con prontitud para retirar la información o hacer que el acceso a ella sea imposible en cuanto tenga conocimiento efectivo de uno de los hechos siguientes:*
· La información ha sido retirada del lugar de la red en que se encontraba inicialmente.
· Se ha hecho imposible acceder a dicha información o
· La autoridad competente ha ordenado retirar esta información o ha prohibido que se acceda a ella."

No obstante esta exención, el artículo 13 de la propuesta, al igual que en el caso de mero transporte, no excluye la posibilidad de una acción de cesación.

(3) Alojamiento de datos. El artículo 14 de la propuesta de Directiva limita la responsabilidad del prestador del servicio en lo que se refiere a la actividad de alojamiento de datos facilitados por el destinatario del servicio (por ejemplo, el suministro de espacio en un servidor para un foro de discusión, para un sitio web de un particular o de una empresa, para un tablón de anuncios electrónico). Salvo en el marco de una acción de cesación, la exención de responsabilidad civil y penal sólo podrá concederse en alguna de las circunstancias siguientes: (a) El prestador del servicio no tiene conocimiento real de que el usuario del servicio ejerce una actividad que revele su carácter ilícito; (b) El prestador del servicio tiene conocimiento de los hechos y circunstancias que demuestran la existencia de una actividad ilícita y actúa con rapidez para retirar los datos o hacer que el acceso a ellos sea imposible. Con respecto a este supuesto, la Comisión fomenta la creación de sistemas de autorregulación incluidos los códigos de conducta.

Esta exención, no obstante, no será de aplicación cuando el destinatario del servicio actúa bajo la autoridad o control del prestador del servicio.

(4) No existencia de obligación de supervisión. La propuesta de Directiva no contempla la imposición a los prestadores de servicios de una obligación general de supervisar o de controlar de forma activa el contenido de las informaciones de terceros. Ahora bien, esta regla no excluye la posibilidad de que la autoridad judicial solicite al prestador del servicio una actividad de supervisión selectiva y transitoria siempre que resulte necesario para garantizar la seguridad del Estado, la defensa, la seguridad pública y para prevenir, investigar, detectar y perseguir infracciones penales.

5. Aplicación de las normativas

Para finalizar, en la propuesta de Directiva, la Comisión, en lugar de establecer nuevas disposiciones legales, pretende asegurar la utilización efectiva de la normativa comunitaria y de las legislaciones nacionales existentes. Esta aplicación se considera básica para generar la confianza mutua entre los Estados miembros, necesaria para la generación de un mercado interior real.

Esta finalidad se puede obtener mediante la consolidación de los mecanismos jurídicos necesarios que, según la propuesta, se refieren a (1) la elaboración de códigos de conducta a escala comunitaria, (2) la potenciación de la cooperación administrativa entre los Estados miembros, (3) la creación de sistemas eficaces para la solución de las divergencias y litigios transfronterizos, y (4) la instauración de un sistema de recurso judicial rápido y efectivo, adecuado al entorno en línea.

6. Conclusión

Las medidas previstas en la presente Directiva se refieren al mínimo necesario para conseguir el objetivo de un correcto funcionamiento del mercado interior dentro del ámbito de la Sociedad de la Información garantizando, en todo caso, la protección de los objetivos de interés general y, en concreto, de la protección del consumidor y la salud pública.

7. Notas

[1] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, 18-I-1998, COM (1998) 598 final.
[2] Esta definición ha sido adoptada por la Directiva 98/34/CE del Parlamento Europeo y del Consejo, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, DO L 204 de 21-VII-1998, modificada por la Directiva 98/48/CE del Parlamento Europeo y del Consejo, 20-VII-1998 que modifica la Directiva 98/34/CE, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, DO L 217, 5-VIII-1998.
[3] Directiva 97/13/CE del Parlamento Europeo y del Consejo, de 10-IV-1997, relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones, DOCE, L 117, 7-V-1997, p.15
[4] Esta obligación de información se suma alas existentes en las legislaciones nacionales y en la Directiva 97/7/CE sobre la protección de los consumidores en materia de contratos a distancia [DOCE, L, 144, 4-VI-1997]
[5] Ibid.
[6] Directiva 97/66/CE de 15-XII-1997, DOCE L 24, 30-I-1998.
[7] Véase, JULIA-BARCELO, R., *"Liability for on-line intermediaries: A European Perspective"*, European Intellectual Prperty Review, vol.20, issue 12, December 1998, pages 453-463.

LegisTIC

Consideraciones jurídicas sobre el denominado "efecto 2000"

Javier Cavestany
Estudio Legal

<javier.cavestany@es.pwcglobal.com>

Publicado en el número de Noviembre-Diciembre de 1998 de OTRO-SÍ, revista del Ilustre Colegio de Abogados de Madrid

Existe un importante número de productos y sistemas informáticos que resultan incapaces de reconocer el cambio de siglo que se acerca, al haber sido desarrollados sobre la base de antiguos programas carentes de los campos de cifras precisos para la total identificación de cada año. Así, el presente año es concebido por tales sistemas como "98", el próximo como "99" y el año 2000, simplemente como "00". Ante esta última cifra, que informáticamente podría llegar a traducirse por "1900", los ordenadores en cuestión pueden dejar de funcionar correctamente, desbaratar la contabilidad de una empresa, desconectar motores por entender que han estado todo un siglo en funcionamiento sin revisión, interrumpir el pago de pensiones o cualesquiera emolumentos o retribuciones ... En definitiva, un problema técnico aparentemente sencillo, derivado de la escasez de recursos de memoria en los antiguos ordenadores, así como de una cierta falta de previsión, ha hecho encender luces de alarma en todos los ámbitos informatizados del mundo ante el caos que se avecina. Este latente problema es conocido como "efecto 2000".

La situación obliga a las administraciones, empresas públicas o privadas y a cualquier particular potencialmente afectado, a adoptar con carácter urgente las medidas técnicas oportunas para evitar, en la medida de lo posible, los perjuicios que en los respectivos ámbitos o frente a terceros, pudiera ocasionar el desbarajuste informático que derivará del "efecto 2000".

En aquellos supuestos en que la falta de previsión o la insuficiencia de medios den lugar al acaecimiento de problemas de funcionamiento de los equipos, a consecuencia del "efecto 2000", que se traduzcan en perjuicios para el propio poseedor o para terceros, será preciso determinar jurídicamente la imputación y extensión de las subsiguientes responsabilidades mediante un pormenorizado análisis de la situación de hecho y sus posibles consecuencias jurídicas. En el presente artículo, sin pretender desarrollar una exégesis extensa de las diversas disposiciones legales y teorías susceptibles de aplicación, realizaremos no obstante una mera aproximación de los distintos resortes que el Derecho podría poner a nuestra disposición en cualquier posible litigio que se suscitara con ocasión del "efecto 2000".

En primer lugar será preciso delimitar si el daño ha sido ocasionado en el ámbito contractual o en el ámbito extracontractual. Es decir, si el perjudicado por el efecto 2000 se encuentra vinculado con el fabricante o suministrador del producto mediante la suscripción de un contrato -que generalmente será de compraventa, suministro, *leasing* o cualquiera otro traslativo de la propiedad del producto o mediante el cual se ceda su uso-, o si el daño ha sido ocasionado sin la preexistencia de vinculo jurídico alguno entre el causante y el perjudicado.

En el ámbito contractual, resulta evidente que los acuerdos específicos alcanzados por las partes tendrán indudable fuerza jurídica para exigir la reparación de los perjuicios causados, si el sistema de garantías o responsabilidades que hubiere sido eventualmente consignado en el clausulado establece con mayor o menor claridad la extensión y límites de las obligaciones asumidas por la parte causante del daño.

Pero aún sin la claridad debida, o en defecto de previsiones específicas para el "efecto 2000", no se debe olvidar que los contratos no sólo obligan a lo expresamente pactado, conforme establece el **artículo 1.258** del **Código civil**, sino que el vínculo jurídico se extiende al desarrollo de las actuaciones complementarias que requiera la buena fe, la costumbre y la ley. En este sentido, si una empresa es consciente de la existencia de riesgos para determinado cliente, a consecuencia de un producto vendido viciado por el "efecto 2000", la buena fe pudiera exigir una intervención activa, bien advirtiendo expresamente, bien facilitando los medios precisos para evitar el daño, en la medida en que ello sea posible.

En cualquier caso, si algún daño es ocasionado en el ámbito de ejecución de una obligación contractual, la responsabilidad subsiguiente, conforme al **artículo 1.101** del Código civil, se extiende a la obligación de indemnizar los daños y perjuicios ocasionados, siempre que el causante hubiere incurrido en dolo, negligencia o morosidad, o en cualquier forma hubiere contravenido el tenor de la obligación originalmente asumida.

La graduación de la culpa en que se pueda haber incurrido en la comercialización de un producto viciado por el problema del "efecto 2000" será en la práctica un extremo de difícil determinación, en el que sin duda la redacción específica del clausulado del contrato suscrito, el fin u objeto del mismo e, incluso, sus elementos accesorios, tendrán gran importancia para determinar si el contratante causante del daño ha cumplido diligentemente sus obligaciones o, en caso contrario, si ha de indemnizar los perjuicios ocasionados por el "efecto 2000", como también lo tendrá la formación o experiencia profesional de la otra parte contratante

En atención a que en la actualidad el "efecto 2000" es conocido por todo productor de sistemas y equipos informáticos, la buena fe contractual exige advertir en forma clara si el producto vendido se puede ver afectado por tal problema. Ocultar dicha información favorecerá cualquier demanda de responsabilidad que el perjudicado pueda instar.

Respecto de productos vendidos en el pasado, afectados por el problema y sin que se haya realizado advertencia alguna por el contratante vendedor o transmitente, cabría considerar que el perjudicado empleara alguna de las siguientes tesis en defensa de sus intereses:
a) Considerar que el producto está afectado por vicios o defectos ocultos.

Hay que tener en cuenta que la acción de saneamiento por defectos ocultos de la cosa vendida, tiene un plazo de vigencia excesivamente breve, como para poder considerar su aplicación a gran escala ante el efecto 2000 (si la compra es calificada como civil, la vigencia de la acción es de 6 meses, contados desde la fecha de entrega).

Por otro lado, podría entenderse que las especiales características del "efecto 2000", no implicarán necesariamente su catalogación como vicio oculto, por cuanto se trataría de una característica común en innumerables equipos y sistemas de similar naturaleza.

Esto es, más que admitir la posible existencia de vicios o defectos ocultos, cabría considerar que el "efecto 2000" consiste en una característica intrínseca del propio producto, a pesar de sus nefastas consecuencias.

b) Entender que el vendedor del producto afectado ha actuado dolosamente al ocultar al adquirente la existencia del defecto o, en su caso, que el adquirente actuó mediando error en su consentimiento, al ignorar tal defecto.

Tanto el dolo como el error -en su consideración exclusiva de vicios del consentimiento a la hora de celebrar un contrato-, acarrearían como consecuencia la nulidad del contrato. Si se aprecia dolo, se deberían asimismo satisfacer los daños y perjuicios causados.

La regulación específica realizada por nuestro sistema legal del saneamiento por vicios ocultos, supone una especialidad respecto de los supuestos de nulidad por error o dolo. Por tanto, sin excluir la posible existencia de pretensiones indemnizatorias basadas en esta teoría, sus posibilidades de éxito serían muy limitadas.

c) El perjudicado por el defecto, podría intentar mantener que el transmitente del producto ha incumplido el contrato, exigiendo, consecuentemente, bien la resolución del contrato o bien el cumplimiento forzoso -reparación del "efecto 2000"-, con indemnización de daños y perjuicios.

Esta posibilidad es realmente difícil si el producto vendido cumple en todos sus demás aspectos los niveles de calidad adecuados. Como habíamos señalado con anterioridad, las eventuales consecuencias del "efecto 2000", podrían alcanzar a terceros ajenos a cualquier vínculo jurídico con el fabricante o poseedor del bien que originó el daño. En tales supuestos, cabría considerar la aplicación del principio de responsabilidad extracontractual recogido en el **artículo 1.902** del Código civil: *"El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".*

No obstante el carácter predominantemente subjetivo de la responsabilidad prevista en el aludido precepto, es preciso recordar que la jurisprudencia ha venido matizando dicho principio, apreciando cada vez en mayor medida la posibilidad de aplicar un principio de responsabilidad objetiva, es decir, imputación de responsabilidades a quien ocasiona el daño, aún cuando haya actuado con la diligencia debida. En otras palabras, quien crea un riesgo en el desarrollo de una actividad económicamente provechosa, ha de soportar los daños que deriven de esa actividad, aún cuando se haya actuado en el más estricto cumplimiento de la normativa aplicable.

Reflejo de esta teoría es el sistema de responsabilidad objetiva que ha inspirado la **Ley 22/1994**, de responsabilidad civil por los daños causados por productos defectuosos. Al encontrarse dicha Ley inspirada en la defensa de los intereses de los consumidores y usuarios, su ámbito estricto de aplicación bien pudiera parecer limitado, si bien no debe obviarse la potencial influencia que los criterios contenidos en la misma pudieran ejercer en otros ámbitos del Derecho, como pueda ser el de las obligaciones puramente extracontractuales.

El principio general de responsabilidad por defecto del producto, a que hemos hecho referencia, se encuentra recogido en el **artículo 1** de la **Ley 22/1994**, que dispone: *"Los fabricantes y los importadores serán responsables, conforme a lo dispuesto en esta Ley, de los daños causados por los defectos de los productos que, respectivamente, fabriquen o importen".*

La mencionada Ley pudiera ser importante en un supuesto como el del "efecto 2000", si bien, en nuestra opinión, la especialidad del problema podría en muchos casos dejar inoperantes las previsiones que en ella se establecen.

La imputación de responsabilidad es efectuada por la Ley a las empresas o entidades que en cada caso tengan el carácter de empresario, importador o suministrador. Esto no obstante, es preciso tener en cuenta que de conformidad con la Legislación en materia de Sociedades Anónimas y Sociedades de Responsabilidad Limitada, los administradores o directivos de estas entidades podrían, en determinadas circunstancias, llegar a sufrir personalmente las consecuencias de eventuales reclamaciones por los daños producidos.

A los efectos de la Ley, por "producto defectuoso" se entenderá aquél que no ofrezca la seguridad que cabría legítimamente esperar, teniendo en cuenta todas las circunstancias y, especialmente, su presentación, el uso razona-

blemente previsible del mismo y el momento de su puesta en circulación.

En todo caso, un producto es defectuoso si no ofrece la seguridad normalmente ofrecida por los demás ejemplares de la misma serie.

El régimen de responsabilidad civil previsto en la Ley, comprende los supuestos de muerte y las lesiones corporales así como los daños causados en cosas distintas del propio producto defectuoso, siempre que la cosa dañada se halle objetivamente destinada al uso o consumo privados y en tal concepto haya sido utilizada principalmente por el perjudicado. En este último caso se deducirá una franquicia de 65.000.- pesetas.

Por otro lado, es preciso indicar que la responsabilidad civil global del fabricante o importador por muerte y lesiones personales causadas por productos idénticos que presenten el mismo defecto tendrá como límite la cuantía de 10.500.000.000.- pesetas.

La exclusión implícita que realiza la Ley respecto de los supuestos no contemplados, no significa que los perjudicados carezcan de acción contra el fabricante para exigir las responsabilidades que pudieran corresponder. La fundamentación de dicha acción habrá de descansar en otras disposiciones normativas y principios generales igualmente válidos (culpa extracontractual), si bien, careciendo de la relativa seguridad que para cualquier pretensión indemnizatoria otorga el respaldo de una ley expresa como la que ahora nos ocupa.

Respecto del elenco de causas de exoneración de responsabilidad que prevé la Ley, cabe destacar aquella que consiste en que el estado de conocimientos científicos y técnicos existentes en el momento de la puesta en circulación no permitía apreciar la existencia del defecto.

Esta causa de exoneración podrá ser adecuada, según las circunstancias, a los fines de servir de base para defender los intereses del fabricante o suministrador frente a eventuales demandas de indemnización basadas en esta Ley.

Dicha defensa parece abordable tratándose de productos fabricados con anterioridad a las fechas en que se conoció o divulgó la existencia del "efecto 2000".

Tratándose de productos fabricados con posterioridad a dichas fechas, las posibilidades de defensa se verían en gran medida disminuidas, si bien no anuladas, por cuanto cabría la posibilidad de argumentar que los componentes utilizados en la elaboración del bien, se encuentran afectados por haber sido fabricados o por depender de aplicaciones elaboradas con anterioridad a tales fechas.

Con independencia de las diversas teorías que hemos expuesto, hay que reconocer la dificultad de predecir el encaje que los daños causados a consecuencia del "efecto 2000" tendrá ante la multiplicidad supuestos de hecho y de fundamentaciones jurídicas susceptibles de aplicación. Pero, en cualquier caso, la novedad del problema no debe hacer olvidar que la fuerza omnicomprensiva de nuestro ordenamiento jurídico, tan enraizado en el antiguo Derecho Romano, ha venido aportando a través de los tiempos soluciones pretendidamente justas a cuantas nuevas cuestiones o supuestos de hecho la realidad ha sometido a la consideración de los Jueces y Tribunales.

Ese carácter en cierta medida "elástico" del Derecho y sus principios generales, será nuevamente puesto a prueba cuando, con el cambio de milenio, las consecuencias del denominado "efecto 2000" se hagan patentes.

Así, los viejos conceptos de culpa, dolo, error, buena fe, responsabilidad contractual o extracontractual, responsabilidad objetiva o subjetiva y tantos otros, serían nuevamente utilizados ante los tribunales para encontrar una solución jurídicamente correcta a un problema inimaginable cuando tales conceptos nacieron.

Pero es precisamente la novedad del problema, su carácter universal, consecuencia de un desarrollo tecnológico que a todos beneficia, y el hecho de que afecte a muy diversos sistemas informáticos, equipos o maquinaria, lo que podría implicar que el juzgador llegara a atemperar sus tradicionales criterios de atribución de responsabilidad, con la finalidad de no obtener un resultado contrario al bien común.

En cualquier caso, y por lo que pudiera suceder, sería muy recomendable que, hasta que el siglo XX llegue a su fin, tanto los adquirentes de equipos potencialmente viciados por el problema del "efecto 2000", como los fabricantes y los vendedores, actuaran ya con la mayor diligencia y buena fe con el fin primordial de evitar o minimizar los daños que tal fallo pudiera ocasionar, todo ello sin olvidar que, en cuanto se refiere a los fabricantes o transmitentes del equipo, tales actuaciones podrían suponer un importante factor de defensa de su posición ante eventuales demandas.

A tales fines, sería preciso realizar no sólo un examen técnico de los equipos informáticos implicados, sino también una revisión pormenorizada de los contratos que sirvieron de base a la transmisión de aquellos, con especial análisis de las cláusulas de garantía o responsabilidad que pudieran incluir.

Del análisis de la situación fáctica y jurídica de cada supuesto, la prudencia y buen criterio comercial pudieran recomendar la adopción de medidas inmediatas, sin esperar al cambio de siglo, y sin descartar la posibilidad de colaboración directa con los potenciales afectados.

LegisTIC

Material de consulta

Emilio del Peso Navarro, Rafael Fernández Calvo

Como complemento de la monografía, recogemos aquí, *sin pretensiones de exhaustividad*, una serie de publicaciones y sitios web relacionados, de forma directa o indirecta, con Legislación y Etica sobre Tecnologías de la Información y de las Comunicaciones, y que consideramos de interés para nuestros lectores.

Bibliografía

Barriuso Ruíz, Carlos. *La contratación electrónica.* Dykinson. Madrid 1998.
Barutel Manaut, Carles. *Las tarjetas de pago y crédito.* Bosch. Barcelona 1997.
Carrascosa López, Valentín; Pozo Arranz, Mª A. y Rodríguez de Castro E.P. *La contratación informática: el nuevo horizonte contractual.* Editorial Comares. Granada 1997.
Comercio Eléctrónico; monografía de Novática nº 135 (Septiembre-Octubre 1998) .
Davara Rodríguez, Miguel Ángel.
- *De las autopistas de la información a la Sociedad Virtual.* Aranzadi. Pamplona, 1996.
- La protección de datos en Europa. *ASNEF-Equifax y Universidad Pontificia Comillas ICADE. Madrid, 1998.*
- Manual de Derecho Informático. *Aranzadi. Pamplona, 1997.*
Fernández Calvo, Rafael. *El ciberespacio y sus dilemas.* El País, 5 de Noviembre de 1996, Especial SIMO (puede obtenerse también en *http://www.elpais.es).*
Fernández Masiá y otros. *Los derechos de propiedad intelectual en la nueva sociedad de la información. Editorial Comares. Granada, 1996.*
Galindo Ayuda, Fernando. *Derecho e Informática.* La Ley, Actualidad. Madrid, 1998.
Gete-Alonso y Calera, María del Carmen. *El pago mediante tarjeta de crédito.* La Ley. Madrid, 1990.
Gutierrez Francés, María Luz. *Fraude informático y estafa.* Ministerio Justicia. Madrid, 1991.
Hernando, Isabel. *Productos Multimedia y derechos de autor.* Editorial LC. San Sebastián, 1997.
Contratos informáticos. *Editorial LC. San Sebastián, 1995.*
Hubin J. Y Poulet, Yves. *La sécurité informatique entré technique et droit.* E. Story-Scientia. Namur, 1995.
Huxley Aldoux. *Un mundo feliz.* Circulo de Lectores. Barcelona, 1965.
Lointier, Pascal. *Internet pour les juristes.* Dalloz, 1996.
Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD). BOE del 31 de octubre de 1992, núm. 262.
Lopez Garrido D., García Arán M. *El Nuevo Código Penal y la voluntad del legislador.* Eurojuris, Madrid,1996.
Morant Ramon, José Luis; Ribagorda Garnacho, Arturo y Sancho Rodríguez, Justo. *Seguridad y protección de la información.* Ramón Areces. Madrid, 1994.
Negroponte, Nicholas. *Mundo Digital.* Editorial B, Madrid, 1996.
Orwell, George. *1984.* Destino. Barcelona, 1987.
Paez Mañá, Jorge. *Bases de Datos Jurídicas.* CSIC. CINDOC. Madrid, 1994.
Pastor Franco, José y Sarasa López, Miguel Ángel. *Criptografía digital. Fundamentos y aplicaciones.* Prensas Universitarias de Zaragoza. Zaragoza, 1998.
Peso Navarro, Emilio y Ramos González, Miguel Ángel. *LORTAD.* *Análisis de la Ley.* Díaz de Santos. Madrid, 1998.
Peso Navarro, Emilio; Ramos González, Miguel Ángel; Fernández Sánchez, Carlos Manuel e Ignoto Azaustre, María José. *Manual de Dictámenes y Peritajes Informáticos.* Díaz de Santos. Madrid, 1995.
Ribas Alejandro, Javier. *Aspectos jurídicos del Comercio Electrónico en Internet.* Aranzadi. Pamplona, 1998.
Saéz Vacas F. *Inforpistas inteligentes.* Editorial América Ibérica. Madrid, 1996.
Sieber Ulrich (edt). *Information Technology Crime.* Carl Heymanns Verlag. K.C. Köln, 1994.
Tapper Colin. *Computer Law.* Longman. England, 1989.
Zamiatin, Yevgueni. *Nosotros.* Tusquets. Barcelona, 1991.

Sitios web:

Legislación
Àrea de Dret civil de la Universitat de Girona*: http://civil.udg.es/*
Boletin Hispanoamericano de Informática y Derecho: *http://members.theglobe.com/boletin/*
CEDIB (Centro de Estudios de Derecho e informática de Baleares)*: http://www.uib.es/depart/dpr/cedibcas.html*
CRDI (*Centre de Recherches Informatique et Droit*), Faculté de Droit, Université de Namur: *http://www.droit. fundp.ac.be/liens/default.htm*
CPSR (*Computer Professionals for Social Responsability*) *Computer Crime and Legal Resource Directory**: http://www.cpsr.org/cpsr/privacy/crime/crime.html*
ECLIP (*Electronic Commerce Legal Issues Platform*), ESPRIT IV Project EP 27028: *http://www.jura.uni-muenster.de/eclip/*
EULISP (*European Legal Informatics Study Programme*): *http://www.eulisp.uni-hannover.de/*
EUR-Lex, el Derecho de la Unión Europea*:* *http://europa.eu.int/eur-lex/es/index.html*
FindLaw (legislative search engine): Legal Subjects: Cyberspace Law: http://www.findlaw.com/01topics/10cyberspace/index.html
Instituto de Informática Jurídica, ICADE, Madrid*: http://www.upco.es/pagnew/titulos/infjur/portada.htm*
Paladella Salord, Carlos de. Páginas sobre Derecho y Tecnología: *http://members.xoom.com/_XOOM/cpaladella/index.htm*
Porras Quintela, Manuel. Páginas sobre Derecho, Informática y Tecnologías de la Información y Comunicaciones: *http://www.ctv.es/USERS/mpq/principal.html*
Ribas, Javier. Legislación sobre TIC: *http://www.onnet.es/leyes.htm*
Seminario Informática y Derecho, Universidad de Zaragoza: *http://www.unizar.es/DERECHO/FYD/INDEX.HTM*
Thomas. *USA Legislative Information on the Internet: http://thomas.loc.gov/*
United Nations. *Manual on the prevention and control of computer-related crime: http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html*

Etica Profesional:
ACM (*Association for Computer Machiner*). *Code of Ethics and Professional Conduct: http://www.acm.org/constitution/code.html*
ACM. *Software Engineering Code of Ethics and Professional Practice. http://www.acm.org/serving/se/code.htm*
ACM. *Computing and Public Policy: http://www.acm.org/serving/*
ACS (*Australian Computer Society*). *Code of Ethics: http://www.acs.org.au/national/pospaper/acs131.htm*
AIP (*Associazione Informatici Professionisti*). *Codice Deontologico degli Informatici Professionisti: http://www.a-i-p.it/info/cod_deon.html*
ATInet: Código de Conducta para usuarios*: http://www.ati.es/socios/introATInet.html*
BCS (*British Computer Society*). *Code of Conduct: http://www.bcs.org.uk/aboutbcs/coc.htm*
BCS. *Code of Practice: http://www.bcs.org.uk/aboutbcs/cop.htm*
Centre for Applied Ethics*: Computer Ethics Resources on WWW:* *http://www.ethics.ubc.ca/papers/computer.html*
CEPIS (*Council of European Professional Informatic Soceities*). *Code of Conduct: http://www.cepis.org/conduct.htm* (ver traducción al castellano en esta misma monografía)
GI (*Gesellschaft für Informatik*) *Ethische Leitlinien: http://www.gi-ev.de/uebersicht/ethische_leitlinien.html*
IEEE (*Institute of Electrical and Electronic Engineers*) *Code of Ethics: http://www4.ncsu.edu/unity/users/j/jherkert/ethics.html*
IFIP *(International Federation for Information Processing)* *Harmonization of Professional Standards: http://www.ifip.or.at /minutes/C99/C99_harmonization.htm*
WWW Ethics Center: *Codes Of Ethics And Conduct: http://www.cwru.edu/affil/wwwethics/codes.html*

Otros:
Agencia de Protección de Datos: *http://www.ag-protecciondatos.es*
Alvarez Marañón, Gonzalo. Páginas sobre amenazas a la privacidad y medios para defenderla: *http://www.iec.csic.es/criptonomicon/*
CNIL (*Commission Nationale de l'Informatique et des Libertés*), Francia: *http://www.cnil.fr/*
DGXIII *at the European Commission:* *http://europa.eu.int/comm/dg13/index.htm*
EFF (*Electronic Frontier Foundation*): *http://www.eff.org*
EPIC (*Electronic Privacy Information Center*): *http://www.epic.org/*
OSTP (*White House Office of Science and Technology Policy*): *http://www.whitehouse.gov/OSTP.html*