Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Protección del consumidor y del usuario en Internet

Laura Gismera Tierno

Universidad Pontificia Comillas de Madrid (ICAI-ICADE)

I. Introducción.

En el estudio de la protección o desprotección del consumidor y del usuario en Internet se ha optado por analizar la vía legislativa, la cual entra a formar parte del panorama ético en su conjunto. Recordemos que la ética se concibe como la suma de principios y valores de carácter moral pero también de normas, de leyes positivas.

Algunos de los problemas concretos que se presentan en Internet en lo referente a la "desprotección" del consumidor son la inseguridad de las transacciones y medios de pago electrónico, la posible invalidez de los contratos, la falta de protección al consumidor en su condición de adquiriente de bienes y servicios, los fraudes documentales, las transacciones ilegales, la falta de protección de la privacidad, de los derechos de propiedad intelectual y de los datos personales. Desde la perspectiva de la "desprotección" del usuario conviene analizar la existencia de pornografía infantil en la Red (especialmente la influencia que ésta puede tener para los menores) y los ciberdelitos desde la perspectiva de la piratería virtual.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico aboga por la protección del consumidor desde diversos puntos de vista.

II. Legislación aplicable a Internet.

La legislación aplicable al caso de la protección de los derechos de los consumidores varía sensiblemente de unos países a otros y por ello es necesario conocer la normativa vigente en el país en el que se encuentra el consumidor. Así por ejemplo el tratamiento de la publicidad dedicada a los menores de edad tiene enfoques restrictivos o permisivos dependiendo del país.

Desde la perspectiva jurídica, las razones que aconsejan un tratamiento normativo del comercio electrónico vienen dadas por la necesidad de generar seguridad en la utilización de esas vías e infundir confianza en su uso al consumidor[1]. Para la resolución de conflictos que plantee cualquier consumidor europeo existen dos vías posibles: la vía judicial (decisión de diciembre de 2000 del Consejo de la Unión Europea sobre jurisdicción y reconocimiento de juzgados en asuntos comerciales y civiles) o la vía extrajudicial (pues la vía de no recurrir a los tribunales de justicia permite reducir costes y tiempo en la resolución de conflictos).

Algunos de los problemas concretos que pueden presentarse en Internet en lo referente a la "desprotección" del consumidor son la inseguridad de las transacciones y medios de pago electrónico, la posible invalidez de los contratos, la falta de protección al consumidor en su condición de adquiriente de bienes y

[1] Egusquiza, M. A. (2000), "Comercio electrónico, intimidad y derechos de los consumidores"·. *Jornadas sobre protección de la privacidad: Telecomunicaciones e Internet*. Pamplona, 22 y 23 de junio.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

servicios, los fraudes documentales, las transacciones ilegales, la falta de protección de la privacidad, de los derechos de propiedad intelectual y de los datos personales.

Entre los problemas concretos subyace el concepto de intimidad. La intimidad es un concepto amplio y, de alguna manera, difícil de formular. La intimidad es necesaria para una diversidad de relaciones, es un aspecto esencial de la autonomía. Sin embargo, es necesario proteger algunos acontecimientos de la vida de una persona contra la publicación, como un precedente para el tratamiento de la cuestión de la información personal almacenada en un ordenador. El derecho común reconoce el derecho del individuo a su personalidad inviolable y que ésta incluye los hechos de su vida.

Este derecho a una personalidad inviolable está estrechamente relacionado con la idea de Kant sobre los humanos como seres autónomos y el respeto que se les debe como tales. La conexión entre la autonomía y la información sobre la persona se hace evidente al fijarnos en las relaciones sociales.

Por todo ellos vamos a centrarnos en cinco grandes bloques a la hora de analizar la legislación aplicable a Internet: contratación digital, protección de datos confidenciales, protección del derecho de propiedad intelectual, pornografía infantil y ciberdelitos en general. La protección de la esfera de la vida privada del individuo (tutela de la privacidad e intimidad) es la base fundamental en todo planteamiento que aquí se realice.

II. 1. Contratación digital.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

El derecho de la contratación a través de Internet afecta al derecho mercantil, derecho internacional privado, derecho procesal, derecho penal, derecho administrativo y derecho tributario. Por ello para analizar la legislación en lo referente a contratación digital hay que estudiar los principios de la contratación electrónica, la dimensión procesal de la prueba del contrato y del documento electrónico, la firma digital y el derecho de la Unión Europea sobre comercio electrónico, los servicios financieros en Internet, las relaciones telemáticas con la administración pública y la tributación del comercio electrónico.

Si se analiza pormenorizadamente el sistema de contratación electrónica quedan resueltas dudas tales como qué es exactamente un contrato celebrado por vía electrónica, si son jurídicamente seguras las operaciones telemáticas, qué derechos y garantías tiene el consumidor o qué impuestos gravan las transacciones por Internet[2]. El apretón de manos fue sustituido por el papel y ahora este es sustituido por el soporte electrónico: por lo tanto, si el medio ha cambiado la legislación ha de seguir las pautas que marca el cambio de infraestructura. Partimos del hecho de que existe el puro consentimiento electrónico que tiene validez legal, es decir, puede existir la perfección consensual de contrato telemático[3].

El objetivo básico de esta legislación es la protección de la intimidad personal y los derechos de los consumidores y para ello:

[2] Mateu de Ros, R. (2000). *Derecho de Internet. Contratación Electrónica y Firma digital*. Pamplona: Editorial Aranzadi, p. 20.

[3] "También existen cláusulas abusivas dentro de los contratos que se perfeccionan a través de Internet, ya que tienen como destinatarios a consumidores y usuarios, no siendo dichas cláusulas abusivas negociadas individualmente. Por tanto, los empresarios que comercializan sus productos o servicios a través de la Red, deberán poner especial cuidado a la hora de incluir cláusulas en sus contratos, porque de no ser así correrán serios riesgos de incorporar estipulaciones que resulten nulas de pleno derecho, y que, por tanto, no podrán ser aplicadas". Expansión, 27 de febrero de 2001. En http://www.abc.es "La Asociación de Internautas demanda a Terra por las cláusulas abusivas de sus contratos de ADSL". Fecha de consulta: 13 de febrero de 2002.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

1. Se identifica al autor de la comunicación electrónica.
2. Se otorga seguridad[4] e integridad al contenido, con la declaración de voluntad "on line" y la secuencia de oferta y aceptación del contrato, teniendo en cuenta que el tráfico electrónico plantea riesgos legales y que deben existir cláusulas de limitación de la responsabilidad y cláusulas para la protección de los datos personales.

Existen varias Directivas de la Unión Europea que regulan distintos aspectos legales relativos a los contratos electrónicos entre empresas. La más importante a este respecto es la *Directiva* (*2000/31/EC*) *del 8 de junio del 2000* sobre "ciertos aspectos legales relacionados con los servicios de la Sociedad de la Información", en concreto el comercio electrónico dentro del mercado interior de los países miembros de la Unión Europea. Esta directiva de comercio electrónico cubre todo tipo de contratos, tanto los contratos entre empresas, y los contratos entre la empresa y el consumidor. Cuando las partes no hayan seleccionado la ley aplicable al contrato, la ley que regirá el contrato será aquella del país que esté más relacionado con el mismo. En la mayoría de los casos, un contrato entre empresas está más relacionado con el país donde está establecido el proveedor del servicio o producto.

II. 1. 1. Anonimato.

Una de las cuestiones a tratar en el tema de contratación digital es el del anonimato. En algunos modelos de negocio el comprador permanece en el anonimato hasta que acepta una de las ofertas. Esto es una indefensión para los proveedores que tienen que tener una garantía, pues el comprador debe tener la solvencia necesaria para

[4] La inseguridad en la Red es quizá el elemento que más frena al comercio electrónico.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

garantizar el pago. Es necesario poder comprobar que el comprador no es insolvente.

También puede ocurrir que el proveedor se encuentre en el anonimato. Así el comprador acepta la oferta en función de sus características sin conocer la identidad del proveedor. Obviamente, el comprador debe fiarse de los proveedores asociados con el "sitio web". Si no existe esa confianza, difícilmente un comprador se decidirá a realizar pedidos utilizando este medio. El anonimato desaparece una vez que alguna de las ofertas es aceptada y es en ese momento cuando comienza la negociación entre las partes.

La posibilidad de efectuar pagos de forma anónima permite aprovechar esta característica para la realización de actividades fuera de la ley. Entre estas actividades se encuentra; 1º. el blanqueo de dinero (un usuario puede esconder el origen de sus ingresos, utilizarlos anónimamente y evitar el pago de impuestos), 2º. la extorsión o chantaje (un usuario extorsionador puede exigir que se le den unas determinadas cantidades que después pueda gastar anónimamente) y 3º. la venta de productos ilegales y la compra de estos productos (el anonimato del comprador permite que un usuario pueda adquirir productos ilegales con la certeza de que no será identificado). Estas tres son las actuaciones de tipo criminal más comunes en la Red favorecidas por el anonimato.

II. 1. 2. Sistemas de pago.

Los sistemas de pago en Internet son los mismos que los sistemas de pago existentes con anterioridad a la aparición de la Red; pago en efectivo, transferencia bancaria, mediante cheque y el pago con tarjeta de débito o de crédito. Lo que

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

diferencia al medio de pago en Internet del tradicional es la velocidad. La efectividad de un sistema de pago electrónico mejora siempre que la velocidad a la que se realizan las transacciones sea mayor que cuando se realizan fuera de Internet.

Otra de las cuestiones a tener en cuenta es que al no haber encuentro físico entre el comprador y el vendedor es necesario que se produzca la autenticación de las partes. También hay que asegurar que ninguna tercera persona tenga acceso a los datos de las partes, es decir, asegurar la integridad de los mismos, al igual que es necesario asegurar el no repudio (que ninguna de las dos partes se eche atrás en el cumplimiento del contrato). Por lo tanto hay tres elementos básicos para al efectividad de los medios de pago tras el contrato electrónico:

1. Autenticación de las partes.
2. Integridad de los datos.
3. No repudio de las partes.

Las Directivas comunitarias que regulan el dinero electrónico son la *Directiva 2000/46/EC del 18 de septiembre de 2000* sobre supervisión de instituciones de dinero electrónico y la Directiva 2000/28/EC del 18 de septiembre de 2000 sobre supervisión de instituciones crediticias.

II. 1. 3. Firma electrónica.

La firma electrónica es un dato infalsificable que asegura que una persona escribió o aceptó el documento en el que se realizó la firma. El receptor puede verificar que el documento tiene como origen la persona dueña de la firma y que no ha sido alterado tras ser firmado. Por tanto, un sistema seguro de firma electrónica necesita de dos

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

métodos: un método para firmar el documento de manera que no sea posible su falsificación, y un método para verificar que una firma es realmente realizada por la persona a la que representa. Más aún, nadie puede repudiar firmas digitales seguras[5]. El firmante del documento no puede desentenderse del mismo declarando que era una falsificación.

La regulación referente a las firmas digitales se recoge en la *Directiva 1999/93/EC del 13 de diciembre de 1999*. Actualmente se puede asegurar que existe una validez de la firma electrónica idéntica para todos los países de la Unión Europea. Con esta directiva la empresa:

1. Está segura de que la persona con la que se está comunicando es quien dice ser.
2. Tiene certeza de que el contenido de la comunicación no se modifica desde que se transmite hasta que se recibe.
3. Evita que un tercero tenga acceso a la información transmitida.
4. Está segura de que si recibe un documento de la persona B, que a su vez lo ha recibido de la persona A, el documento que se recibe es que el que realmente envió la persona A en un principio.

II. 2. Protección de datos.

[5] Cuatro son los requisitos que establece el art. 19 del Real Decreto Ley 14/1999 sobre firma electrónica para considerar a un dispositivo de creación de firma electrónica como "seguro": 1. Que garantice que los datos utilizados para la generación de la firma pueden producirse sólo una vez y que asegure su secreto. 2. Que asegure que esos datos no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente. 3. Que los datos de verificación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros. 4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse no impida que éste se muestre el signatario antes del proceso de la firma.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Las Directivas europeas sobre protección de datos[6] tienen como objetivo permitir el flujo de datos entre los distintos Estados miembros de la Unión Europea, al mismo tiempo que intentan proteger los derechos fundamentales de los individuos y garantizar la confidencialidad de los mensajes enviados, de modo que sólo puedan ser abiertos por el vendedor y el destinatario del mismo[7]. Cada empresa debe implementar mecanismos para la recopilación, utilización y el acceso a esos datos.

En cuanto a los datos de carácter personal[8]:

1. Los datos personales sólo pueden ser recogidos y procesados si ello está explícitamente permitido por la ley o si el cliente da su consentimiento de modo explícito[9].
2. Los datos deben ser utilizados exclusivamente para aquello para lo que fueron recopilados inicialmente[10]. No se podrán enviar a ninguna otra empresa sin el consentimiento del cliente al que pertenecen esos datos[11].

[6] *Directiva de protección de datos de la Unión Europea 95/46/EC del 24 de octubre de 1995* y la *Directiva de protección de datos de las telecomunicaciones 97/66/EC del 15 de diciembre de 1997*.

[7] Juan Manuel Fernández (director de la Agencia de Protección de Datos) advirtió de que un sencillo clic con el ratón del ordenador puede trasladar al usuario de una empresa a otra, que puede estar incluso en otro país del mundo, que no está claramente identificada en la web y que puede utilizar o registrar los datos del cliente sin su previo consentimiento. Aseguró, asimismo que algunas "tiendas virtuales" pueden almacenar los datos de un cliente que abona los productos con su tarjeta, y aseguró que en este sentido se han detectado serios incumplimientos. Cinco Días, 27 de julio de 2001.

[8] La Directiva de protección de datos prohíbe expresamente la transferencia de datos personales a países donde el nivel de protección de datos sea considerado como insuficiente. Los Estados Unidos se encuentran dentro de este tipo de países, ya que la protección de los datos no está regulada, ni existe ninguna oficina federal responsable de este aspecto.

[9] http://www.lavanguardia.es/web/30249257.html, "Hotmail ofrece datos personales a empresas sin el consentimiento de sus usuarios". Microsoft asegura en su web que "no comparte la información personal de su perfil con otras empresas sin su consentimiento previo", y en esto no miente. Sin embargo, Hotmail ha introducido tres casillas en la opción de "Perfil", de las cuales la compañía ha cumplimentado dos según sus intereses. De este modo, si el usuario no descubre estas nuevas casillas y no modifica las preferencias que Microsoft ha rellenado por él, estará compartiendo su dirección de correo electrónico y el resto de su información de registro, es decir, datos como fecha de nacimiento, país y provincia de residencia, edad, accesibilidad u ocupación". Fecha de consulta: 21 de junio de 2002.

[10] http:://www.ictnet.es/esp/servicios/noticias/pronews/internet/4601.htm, "Un error de seguridad puede costar muy caro a la empresa". La Agencia de Protección de Datos ha impuesto multas

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

3. Se deben tomar las medidas de seguridad necesarias para evitar pérdidas accidentales de los datos.
4. Se debe permitir al cliente el acceso para modificar sus datos personales. Debe dársele la posibilidad de borrar los mismos, y ello debe poder hacerse en un tiempo razonable.
5. El cliente tiene el derecho de negarse a que sus datos sean utilizados para el marketing directo. Para ello existen dos sistemas de autorización previa o sistema de negación explícita[12].

La Ley Orgánica 15/1999 sobre Protección de Datos (LOPD) establece una serie de principios a tener en cuenta:

1. Principio de calidad de datos (artículo 4[13]).
2. Principio de finalidad (artículo 4. 2.[14]).
3. Principio de información (artículo 5[15]).

multimillonarias a compañías cuyos datos de clientes o usuarios han quedado expuestos al público. Otro daño grave es de imagen y la desconfianza que genera ver una web asaltada. Fecha de consulta: 19 de julio de 2001.

[11] "Casi la mitad (un 46 por ciento) de las tiendas virtuales inspeccionadas en España por la Agencia de Protección de Datos no usa un canal seguro que garantice la confidencialidad de los datos personales de los compradores por Internet. Entre estos datos suele figurar el código de la tarjeta de crédito con el que se paga la transacción. Otra de las prácticas ilegales detectadas hacen referencia al hecho de que las empresas de comercio electrónico no hayan inscrito en el Registro General de Protección de Datos la existencia de un fichero donde se depositan los datos privados de los usuarios. Un 36 por ciento de las webs analizadas incurre en esta falta (sancionable con hasta 60.000 euros). Un comprador que quiera reclamar por el uso de sus datos no sabe a quién dirigirse". El País, 14 de septiembre de 2001.

[12] En el caso del sistema de autorización previa, el destinatario debe autorizar el envío de correos electrónicos promocionales. Este sistema ha sido el escogido por Dinamarca, Finlandia, Italia, Alemania y Austria. En el sistema de negación explícita, aquellos usuarios que no deseen recibir correos electrónicos promocionales deben especificarlo explícitamente en las listas que existen al efecto.

[13] Los datos de carácter personal sólo se podrán tratar cuando sean adecuados, pertinentes y no excesivos. Se mantendrán exactos y puestos al día o en su caso cancelados.

[14] No podrán usarse los datos para finalidades incompatibles con aquellas para las que hubieran sido recogidas, debiendo haberse recogido para finalidades determinadas, explícitas y legítimas.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

4. Principio de consentimiento[16].
5. Principio de seguridad de los datos[17].

La nueva economía ha potenciado algo que ya existía. El tráfico de información confidencial mueve ahora más dinero que nunca y los datos personales constituyen un activo valioso para los comerciantes, los publicistas y los estrategas del mundo de Internet. Es cierto que el pago de multas es cada e vez más frecuente. Es importante señalar que el 16 de mayo de 2001 la Unión Europea y Estados Unidos estaban alejados en sus planteamientos sobre la protección de datos en Internet.

II. 3. Protección de los derechos de propiedad intelectual.

Según la teoría jurídica de los derechos de propiedad intelectual se considera que un "trabajo creativo" es un tipo de propiedad que confiere al propietario el derecho para utilizarlo, alquilarlo o venderlo. Este derecho le otorga al creador del trabajo unos derechos de exclusividad limitados en el tiempo. Existen varias categorías de

[15] En la recogida de datos hay que informar al ciudadano de la existencia del fichero o tratamiento, de la finalidad de la recogida de los datos y los destinatarios de la información, del carácter obligatorio o facultativo, así como de los derechos de acceso, rectificación, cancelación y oposición.

[16] Salvo situaciones excepcionales (cuando lo disponga una Ley, se derive de una relación contractual o proceda de fuentes accesibles al público) el tratamiento de los datos personales requerirá el consentimiento del afectado, al que la Ley Orgánica de Protección de Datos define como manifestación de voluntad, libre, inequívoca, específica e informada. Ello no obstante no determina que el consentimiento tenga que ser siempre escrito, pues este sólo se exige para una especie de datos especialmente protegidos (los que revelan ideología, religión y creencias), ni siquiera expreso, pero en cambio sí se exige en el supuesto de datos que revelen origen racial, salud y vida sexual. Bastará con carácter general el consentimiento tácito. El problema, en todo caso, se planteará a la hora de probar que se obtuvo el consentimiento de esta forma.

[17] Obliga a la adopción de medidas de índole técnico y organizativo que garanticen la seguridad e integridad de los datos y eviten su alteración, pérdida o acceso no autorizado. El nivel de las medidas que será necesario adoptar dependerá de la categoría de los datos tratados, en los términos que establece el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999 de 11 de junio, que la Ley Orgánica de Protección de Datos expresamente deja en vigor.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

derechos de protección intelectual como son la protección de bases de datos, la protección de diseños industriales y la propiedad industrial (marcas y patentes).

En el caso de los portales, nos interesa la legislación relativa al *copyright*. El *copyright* es un derecho de propiedad intelectual asociado a un trabajo original como puede ser un disco o un libro que controla el derecho de copia del trabajo, con una duración de hasta 70 años después de la muerte del autor. La legislación vigente en el campo del *copyright* es la Convención de Berna y la Directiva del Consejo Europeo del 9 de abril de 2001.

Muchas de las noticias que se incluyen en los portales suelen provenir de agencias de noticias o de medios de comunicación. Un portal tiene dos alternativas: rehacer la noticia o publicarla tal cual. En el segundo caso, es necesario que se mencione con claridad cuál es la fuente de la noticia si este portal no quiere tener problemas de tipo legal. Un dato a tener en cuenta es que con Internet aumenta la capacidad de almacenar un volumen importante de datos y de obras a las que el usuario puede acceder fácilmente[18]; por este motivo todavía es más necesario proteger la propiedad intelectual.

"El desarrollo de la sociedad de la información viene marcado por la búsqueda constante del equilibrio entre tecnología y contenidos. El control, respaldado por la legalidad, del uso de los productos audiovisuales es un elemento fundamental para poder seguir disfrutando de los artistas, de sus emociones, de su capacidad

[18] Del Águila, A. R. y Padilla, A. (2001), *E-business y Comercio Electrónico. Un enfoque estratégico.*Madrid: Editorial Ra-Ma, p. 199. "El caso Napster ha enfrentado a esta firma con empresas discográficas y a dos modelos de negocio o de forma de ver y de actuar en el mundo discográfico. El planteamiento de negocio de Napster se basa en la esencia de Internet: compartir libremente todo aquello que es interés de todos. Napster siempre ha alegado, ante las denuncias que le han sido formuladas, que ellos sólo ponen los medios, pero que son los usuarios los que deciden distribuir los ficheros que tienen almacenados en sus discos duros. Sin embargo, con este proceder lo que ocurre es que la distribución irregular de millones de piezas musicales se convierte en una práctica habitual".

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

creadora, que en ningún caso puede aportar la tecnología a secas: una vez más en la historia de la humanidad volverá a evidenciarse que con la defensa de los derechos de un colectivo (por ejemplo, los artistas) se está evitando la desaparición o la perversión de una cultura que ha llevado siglos mantener y transmitir"[19].

Según Pilar Sánchez-Bleda[20] hay cuatro medidas que se suelen adoptar para proteger los derechos de propiedad intelectual de un web:

1ª. Establecer un "link" dentro de la propia página que tenga como destino un texto en el que se explique la titularidad o licencia de los derechos de propiedad intelectual de todos los elementos integrantes del web y de las prohibiciones de uso. Con la creación de este "link" se pretende que cualquier usuario pueda conocer tales normas y prohibiciones mediante su simple lectura. Este texto se puede poner a disposición de terceros a través de un "link" titulado Propiedad Intelectual o *copyright*, o bien insertarse en unas normas más amplias y que engloban más aspectos, tituladas normalmente normas de acceso y utilización de la web o aviso legal.

2ª. Inscribir en el Registro de la Propiedad Intelectual, al menos, el formato HTML y el código fuente de la página web. El Registro de la Propiedad Intelectual admite las solicitudes de registro de web, e incluso tiene determinados los documentos y requisitos necesarios que deben acompañar tal solicitud.

3ª. Otra alternativa, no excluyente de la anterior, es el depósito notarial de todos los elementos que se han ido analizando y que, en conjunto, componen el web. Se trataría de depositar ante notario los contenidos de la página que ofrece la entidad, su diseño gráfico y el código fuente. Esto supone una ventaja respecto al Registro

[19] http://www.ictnet.es/esp/servicios/noticias/pronews/internet/4664.htm. Fecha de consulta: 8 de agosto de 2001.
[20] http://www.ictnet.es. Cinco Días, 20 de marzo de 2001.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

de la Propiedad Intelectual, ya que en el caso del depósito notarial no se limita el número de documentos que hay que aportar.

4ª. Otra medida adicional para complementar la protección es la utilización de símbolos de advertencia sobre protección de derechos de propiedad intelectual. El símbolo “c” dentro de un círculo supone una especie de publicidad posesoria que puede ser valiosa para la entidad a la hora de intentar demostrar la mala fe del posible imitador, plagiario o, en definitiva, infractor de sus derechos de propiedad intelectual.

Por tanto, la página web, como medio de comunicación, es un elemento en el que confluyen multitud de elementos de la más variada índole y por ello es esencial que la entidad que pretenda una correcta y libre explotación de la misma obtenga la totalidad de los derechos de explotación.

II. 4. La pornografía infantil.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Internet se ha convertido en el nuevo lugar de reunión de los pederastas[21] que intercambian todo tipo de informaciones delictivas a través del correo electrónico, las listas de discusión, las páginas web o los salones de conversación en tiempo real (*chat*) que existen en Internet. Son delincuentes difíciles de localizar porque utilizan los ordenadores de instituciones públicas y se comunican a través de códigos que hacen que su detección sea complicada. Este tipo de delincuentes ya existía en el mundo real, pero Internet permite que el material sea más accesible y su control es más difícil.

En España, la legislación está tipificada en el Código Penal de 1995, reformado por Ley 11/1999 sobre los "delitos relativos a la libertad e indemnidad sexual de los menores", aspectos que habían quedado fuera de la regulación penal. En la actualidad, se sanciona, en el artículo 189 del Código Penal, la comercialización de pornografía infantil con penas de uno a tres años de prisión, independientemente del origen (extranjero o desconocido) del material pornográfico.

II. 5. Los ciberdelitos.

[21] Graham, G. (2001), *Internet. Una indagación filosófica*. Madrid: Grupo Anaya, pp. 122-123. "Existe una fuerte tendencia en el mundo moderno a suponer que el valor bueno o malo de los estados mentales y del carácter radica enteramente en las acciones externas a que dan origen, y esto hace que se tienda a ignorar el carácter esencialmente subjetivo de la pornografía y a discutir su rectitud o su maldad únicamente desde el punto de vista de los daños objetivos que ocasiona o que dicen que ocasiona. Pero podemos fácilmente imaginar el caso de alguien que, digamos, pasa su tiempo buscando y mirando pornografía infantil muy lasciva pero nunca comete acto pedófilo alguno. Desde el punto de visa de los efectos externos, su interés es inofensivo y, por esta razón, mucha gente se preguntaría si realmente hay algo malo en ello. Buena parte de esta misma gente se negaría a decir públicamente que la pornografía infantil toma parte de sus intereses y si alguien lo confiesa por inadvertencia, se convierte en motivo de vergüenza. No obstante, si la única señal de agravio es el daño exterior, ¿de qué habría que avergonzarse? La respuesta es que de nada. Como sí hay algo de lo que avergonzarse, se deduce que el daño exterior no puede ser la única señal de agravio moral. ¿Cuál sería la otra señal? La respuesta es que la revelación de tales aficiones muestra un estado mental y un carácter que son sórdidos, causen o no daño al prójimo".

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Ciberdelito vendría a ser todo delito cometido en la Red; por lo tanto, casi todo lo expuesto anteriormente se considerarán ciberdelitos. Algunos de estos delitos son el espionaje industrial, los sistemas de sabotaje, el robo de datos confidenciales, el fraude, el narcotráfico, la pornografía infantil y el blanqueo de dinero, entre otros.

Se cometen fraudes en subastas (después de enviar su dinero, el comprador recibe un producto de menor valor que el prometido o de ningún valor), timos de proveedores de servicios de Internet, promociones de sitios web (se reciben cargos en la factura de teléfono por servicios que el individuo nunca ha aceptado ni solicitado). Cada día se producen 1.400 robos de documentos de identidad en Internet en Estados Unidos, pues es relativamente sencillo para un ladrón electrónico conseguir el número de la seguridad social de un estadounidense, solicitar con él una tarjeta de crédito y empezar a gastar, puesto que en la Red sólo se necesitan el nombre y apellidos, número de la tarjeta y su fecha de caducidad.

Bryan W. Husted[22] ha analizado los factores y variables de un país que implican un mayor crecimiento de la piratería. La piratería de software está correlacionada perceptiblemente al Producto Interior Bruto per cápita, la desigualdad de la renta y el individualismo. Tanto los programas que impiden la piratería como las sugerencias para que ésta disminuya todavía se están desarrollando.

Según los resultados de un estudio realizado por *Computer Emergency Response Team*, los ciberataques son cada vez más sofisticados y destructivos, mientras que los “cortafuegos” (sistema que se coloca entre una red local e Internet) pierden rápidamente su efectividad contra los intrusos. A finales de los años 90 la falta de legislación facilitó la aparición de la ciberpiratería.

[22] Husted, B. W. (2000), “The impact of National Culture on Software Piracy”, *Journal of Business Ethics*, 26, pp. 197-211.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

"Estamos ante un conflicto de valores. Establecer metas y objetivos, optimizar, ser flexible, mantener la estabilidad, ser laborioso, valorar ante todo el dinero y llevar siempre la contabilidad de resultados son las virtudes básicas del empresario capitalista, como indica el filósofo Peca Imanen en "La ética del *hacker* y el espíritu de la era de la información" comentando a Robbins. Frente a ellos, los *hackers* defienden la pasión, la libertad, el valor social y, sobre todo, la creatividad"[23]. El diccionario del argot *hacker*, el "jargon file", compilado de forma colectiva en la Red, define a los *hackers* como personas que se dedican a "programar de forma entusiasta" y creen que "poner en común la información constituyen un extraordinario bien, y que además para ellos es un deber de naturaleza ética compartir su competencia y pericia elaborando software gratuito y facilitando el acceso a la información y a los recursos de computación siempre que ello sea posible".

Ésta ha sido *la ética hacker* desde que un grupo de programadores del MIT (*Massachussets Institude of Technology*) empezaron a llamarse *hackers* a principios de la década de 1960. Con posterioridad, a mediados de la década de 1980, los medios de comunicación empezaron a aplicar el término a los criminales informáticos. A fin de evitar la confusión con aquellos que dedican su tiempo a escribir virus informáticos y a colarse en los sistemas de información, los *hackers* dedican su trabajo a evitarlo, en defensa de la privacidad en el ciberespacio. En una serie de países, se ha debatido a fondo la llamada "puerta trasera de Internet", el acceso a las identidades de la Red por parte de los gobiernos a fin de extender la vigilancia al ciberespacio cuando así lo estimen necesario, o incluso como mecanismo para el control constante del correo electrónico de la población, y de las pautas de búsqueda en la Red.

[23] Javier Etxeberria, "Ética en Internet". El País, 13 de abril de 2002.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

En este sentido, la diferencia entre los países desarrollados y los que se hallan en vías de desarrollo parece consistir en que en los primeros existe un debate sobre legalidad de estás tácticas, mientras que en los segundos sus gobiernos usan estos dispositivos sin que haya habido ningún debate preliminar.

La eticidad requiere una perspectiva temporal más amplia, es decir, responsabilizarse respecto a las consecuencias futuras de las tendencias dominantes y tener la capacidad de imaginar el mundo de forma diferente a la actual.

II. 6. La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico pretende dotar de una mayor seguridad jurídica a las transacciones realizadas a través de Internet, que tengan carácter comercial o que persigan un fin económico. El objetivo de la ley es, además, impulsar la utilización de la Red como medio para realizar negocios. Tanto los portales como las empresas que realicen actividades a través de Internet, las “páginas web” y, en general, los denominados prestadores de servicios deberán mostrar en un lugar visible de sus “páginas web” cierta información básica como su nombre, el domicilio de su sede social y la dirección de correo electrónico.

Además, estarán obligados a mostrar los precios de los productos que ofrecen. Si la empresa realiza una actividad profesional, deberá informar acerca del cumplimiento de los requisitos a los que esté sometida (por ejemplo, su colegiación). El objetivo es que los usuarios sepan en todo momento con quién están contratando vía Internet.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Por otro lado, las empresas de Internet deberán reforzar las garantías para los usuarios en cuanto a la contratación electrónica. Los internautas podrán disponer de la información relativa a las condiciones generales de la contratación aplicables al contrato "on-line". Además, los prestadores de servicios estarán obligados a guiar al consumidor durante todo el proceso de contratación para ayudarle a completar la compra y deberán confirmarles la recepción de sus petición.

La ley también prohíbe el envío de publicidad no solicitada (*spam*). Además, las empresas de servicios de la sociedad de la información deberán contemplar el aumento de sus obligaciones en relación con la protección de datos personales y la lucha contra la delincuencia virtual.

Un proveedor de servicios de Internet (ISP) no es responsable de los contenidos que "cuelgan" sus clientes, pero "debe adoptar las medidas necesarias para que se interrumpa su prestación o para retirar datos que vulneren la Ley". Esto significa tener que retirar la información ilícita desde el momento en el que conozca su existencia (este aspecto, entre otros, ha sido criticado por los representantes de asociaciones de usuarios de Internet por considerar que establece pautas de control y autocensura a los servidores y les responsabiliza de los contenidos). El gobierno pidió que los proveedores de servicios de Internet (ISP) retuvieran los datos de las comunicaciones electrónicas durante un año, medida necesaria para el éxito de una investigación criminal. Esta medida ha sido modificada para su "puesta a disposición de las autoridades judiciales o policiales" en la investigación de delitos cometidos utilizando Internet (sólo un juez podrá cerrar una "página web").

"La Ley de Servicios de la Información y de Comercio Electrónico viene a regular temas tan polémicos como la presencia de una empresa u organización en Internet, desde aspectos sencillos, como puede ser una simple comunicación comercial,

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

hasta cuestiones más o menos problemáticas que inciden incluso en múltiples relaciones mercantiles, como, por ejemplo, la contratación de bienes o servicios por vía electrónica, el suministro de información por vía telemática o, por no seguir enumerando todos y cada uno de los servicios de la sociedad de la información, el ofrecimiento de instrumentos de búsqueda, acceso y recopilación de datos y transmisión de información a través de una red de telecomunicaciones".[24]

En definitiva, esta ley intenta igualar las actividades económicas en Internet a las tradicionales, prohíbe la publicidad masiva sin permiso previo y fomenta la solución extrajudicial de conflictos.

III. Conclusiones.

Tanto la vía jurídica como ética en lo relativo a la protección del consumidor y del usuario en Internet ya han sido abiertas, bien es cierto que queda mucho camino por recorrer por parte de los distintos países y organismos internacionales.

Algunos de los problemas concretos que se presentan en Internet en lo referente a la "desprotección" del consumidor son la inseguridad de las transacciones y medios de pago electrónico, la posible invalidez de los contratos, la falta de protección al consumidor en su condición de adquiriente de bienes y servicios, los fraudes documentales, las transacciones ilegales, la falta de protección de la privacidad, de los derechos de propiedad intelectual y de los datos personales. Desde la perspectiva de la "desprotección" del usuario conviene analizar la existencia de

[24] Davara, M. A. (2002), "La Ley de Servicios de la información y de Comercio Electrónico", *Otrosí* 41, pp. 38-41.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

pornografía infantil en la Red (especialmente la influencia que ésta puede tener para los menores) y los ciberdelitos desde la perspectiva de la piratería virtual.

No podemos olvidar que Internet cuenta cada vez con más usuarios, tanto particulares como empresas y que requiere de una continua y rápida actualización en todo lo relativo a los sistemas de protección del usuario.

Bibliografía

Del Águila, A. R. y Padilla, A. (2001), E-business y Comercio Electrónico. Un enfoque estratégico. Madrid: Editorial Ra-Ma.

Graham, G. (2001), Internet. Un indagación filosófica. Madrid: Ediciones Cátedra.

Mateu de Ros, R. (2000). Derecho de Internet. Contratación Electrónica y Firma digital. Pamplona: Editorial Aranzadi, p. 20.

Otras fuentes de documentación

Davara, M. A. (2002), “La Ley de Servicios de la información y de Comercio Electrónico”, Otrosí 41, pp. 38-41.

Egusquiza, M. A. (2000), “Comercio electrónico, intimidad y derechos de los consumidores”. *Jornadas sobre protección de la privacidad: Telecomunicaciones e Internet*. Pamplona, 22 y 23 de junio de 2000.

Publicación en línea. Granada (España). Número 3. ISSN: 1695-324X

Husted, B. W. (2000), "The impact of National Culture on Software Piracy", *Journal of Business Ethics,* 26, pp. 197-211.

Directiva de protección de datos de la Unión Europea 95/46/EC del 24 de octubre de 1995.

Directiva de protección de datos de las telecomunicaciones 97/66/EC del 15 de diciembre de 1997.

Ley Orgánica 15/1999 sobre Protección de Datos

Real Decreto Ley 14/1999 sobre Firma Electrónica.

Sitios web consultados

www.abc.es

www.lavanguardia.es

www.ictnet.es