

COMERCIO ELECTRÓNICO EN INTERNET

GUÍA DEL CONSUMIDOR

XAVIER RIBAS ALEJANDRO



Centro Europeo
del Consumidor



EUSKO JAURLARITZA
GOBIERNO VASCO

INDUSTRIA, MERKATARITZA
ETA TURISMO SAILA
Merkatatza eta Kontsumo Salburuordetza

DEPARTAMENTO DE INDUSTRIA,
COMERCIO Y TURISMO
Viceconsejería de Comercio y Consumo

Dpto. de Industria, Comercio y Turismo
Dirección de Consumo
Centro Europeo del Consumidor
C/. Donostia - San Sebastián, 1
01010 Vitoria-Gasteiz
Tels.: +34 945 01 99 48 / +34 945 01 99 23
Fax: +34 945 01 99 47
E-mail: cec@ej-gv.es
<http://www.euskadi.net/consumoinfo>

ÍNDICE

PRÓLOGO	5
CÓMO UTILIZAR ESTA GUÍA	6
1. CONSIDERACIONES GENERALES	7
1.1 Naturaleza del medio utilizado: Internet	7
1.2 El factor decisivo de la distancia	8
1.3 Obstáculos y factores inhibidores	8
1.4 La protección del consumidor a través de Internet	8
1.5 Garantías adicionales: códigos éticos	9
2. ÁREAS ANALIZADAS	11
2.1 Información del comercio	11
2.2 Características del producto o servicio	11
2.3 Marketing y publicidad en Internet	11
2.4 Datos personales	12
2.5 Condiciones generales de contratación	15
2.6 Medios de pago	17
2.7 Fiscalidad	19
2.8 Responsabilidad civil	20
2.9 Resolución de controversias	20
2.10 Fraudes y delitos en Internet	21
3. FICHAS	25
3.1 Información del comercio	25
3.1.1 Indicación de los datos identificadores del comercio	27
3.1.2 Localización geográfica del comercio	28
3.1.3 Autenticación de la identidad del comercio	29
3.2 Características del producto o servicio	31
3.2.1 Indicación de las características del producto	33
3.2.2 Productos ilegales	34
3.2.3 Productos farmacéuticos	36
3.2.4 Productos milagro	37
3.2.5 Productos financieros extranjeros	38
3.3 Marketing y publicidad en Internet	39
3.3.1 Obstáculos para la navegación	41
3.3.2 Publicidad intrusiva	42
3.3.3 Captura de direcciones de correo electrónico	43
3.3.4 Publicidad no solicitada por correo electrónico	45
3.3.5 Publicidad engañosa en Internet	47
3.3.6 Publicidad ofensiva	48
3.3.7 Publicidad encubierta	49
3.3.8 Actos de confusión en buscadores	50
3.3.9 Actos de confusión en páginas web	52

3.4 Datos personales	53
3.4.1 Consentimiento del usuario	55
3.4.2 Ejercicio derechos de acceso, rectificación y cancelación	57
3.4.3 Cesión de datos	58
3.4.4 Cookies	59
3.4.5 Análisis de hábitos de navegación y perfiles	61
3.4.6 Política del comercio respecto a los datos personales	63
3.4.7 Protección de menores	64
3.5 Condiciones generales de contratación	65
3.5.1 Información previa	67
3.5.2 Aceptación mediante "click"	68
3.5.3 Prueba del contenido de las CGC	69
3.5.4 Plazo de entrega	70
3.5.5 Forma de entrega	71
3.5.6 Plazo de desistimiento	72
3.5.7 Devoluciones: requisitos, productos excluidos, gastos	73
3.5.8 Garantías	74
3.5.9 Productos financieros	75
3.6 Medios de pago	77
3.6.1 Pago mediante tarjeta de crédito	79
3.6.2 Servidor seguro	80
3.6.3 Firma electrónica	81
3.6.4 La seguridad y el usuario final	82
3.7 Fiscalidad	83
3.7.1 Fiscalidad directa: retenciones a no residentes	85
3.7.2 Fiscalidad indirecta: I.V.A.	86
3.7.3 Aranceles	87
3.8 Responsabilidad civil	89
3.8.1 Productos defectuosos	91
3.8.2 Transmisión de virus	92
3.8.3 Información no actualizada	93
3.9 Resolución de controversias	95
3.9.1 Arbitraje de consumo	97
3.9.2 Arbitraje especializado en comercio electrónico	98
3.9.3 Cláusulas de sumisión expresa	99
3.10 Fraudes y delitos en Internet	101
3.10.1 Estafas electrónicas	103
3.10.2 Daños informáticos	104
3.10.3 Uso no autorizado de terminales	105
3.10.4 Transferencias de fondos no autorizadas	106
3.10.5 Interceptación de correo electrónico	107
3.10.6 Falsedades documentales	108
4. APÉNDICE LEGISLATIVO	109
5. GLOSARIO DE TÉRMINOS RELACIONADOS CON EL COMERCIO ELECTRÓNICO ...	131
6. LINKS	135

PRÓLOGO

La implantación del comercio de consumo a través de Internet, en su ámbito denominado "Business to Consumer" o B2B, es un hecho innegable, a pesar de la timidez con la que se inició y de los obstáculos y factores inhibidores que todavía actúan como lastre para algunos usuarios.

Puede decirse que en Internet, en este momento, existe más oferta que demanda, y no parece que la población de internautas que se ha calculado en los estudios demográficos más recientes sea capaz de absorber todos los servicios y productos que se ofrecen a través de tiendas virtuales.

Ello implica una mayor competencia y una lucha por obtener el liderazgo del sector que además de traer efectos positivos al usuario, como una reducción sustancial de los precios, puede generar un descenso en la calidad de los productos o del servicio al cliente, además de los efectos derivados de la propia naturaleza del medio utilizado y de las características inherentes a toda venta a distancia.

El Centro Europeo del Consumidor del País Vasco, consciente de la necesidad de sensibilizar al usuario de la red sobre sus derechos como consumidor, ha editado esta guía, cuyo objetivo es delimitar y analizar los principales riesgos jurídicos derivados del comercio electrónico en Internet, apuntando unas recomendaciones que sirvan de apoyo y referencia práctica en el momento de realizar una compra a través de la red.

CÓMO UTILIZAR ESTA GUÍA

Esta guía está dividida en dos partes principales:

- Una introducción en la que se describen los aspectos generales y las características esenciales del comercio electrónico de consumo a través de Internet, y
- Un conjunto de fichas en las que se analiza un riesgo concreto y se apuntan unas recomendaciones para que el usuario pueda minimizarlo al máximo.

Las fichas correspondientes a la segunda parte están estructuradas en las siguientes secciones:

Área analizada: Se describe el área de riesgo y se analizan los factores que pueden generar un perjuicio para el usuario. El origen de dichos riesgos se hallará en algunos casos en la propia red Internet como plataforma en la que se realiza la transacción. En otros casos, se tratará de riesgos genéricos de la venta a distancia y del comercio de consumo en general.

Actividad preventiva: Se plantean cuáles de las medidas que el usuario debe aplicar antes de efectuar la transacción, con el fin de evitar los riesgos derivados del área analizada.

Acciones a realizar: Se proponen los pasos a seguir en el caso de que el usuario considere que se halla ante un riesgo potencial y concreto o haya sufrido un perjuicio específico.

Legislación aplicable y códigos éticos: Se reproducen, en el apéndice legislativo, fragmentos de los textos legales aplicables y de los códigos éticos sectoriales que pueden aportar argumentos y fundamentación legal para la prevención del riesgo o la reparación del daño causado.

1. CONSIDERACIONES GENERALES

1.1 Naturaleza del medio utilizado: Internet

No podemos iniciar el análisis de la protección del consumidor en el comercio electrónico sin valorar previamente las características del entorno en el que van a tener lugar las transacciones electrónicas entre el oferente y el adquirente.

Internet se configura como una gran malla internacional que une millones de ordenadores entre sí, y que ofrece la posibilidad de visualizar el contenido de servidores de información que se hallan a una gran distancia, intercambiar mensajes con otros usuarios y realizar todo tipo de operaciones telemáticas.

El soporte físico de esta red está constituido por unos enlaces de alta velocidad que permiten transportar los datos de un país a otro con tal rapidez e inmediatez que da la impresión de que el usuario está operando en un mercado virtual, ajeno a cualquier vinculación geográfica y desprovisto de fronteras.

Ello genera inmediatamente una incertidumbre respecto a la legislación aplicable y a la jurisdicción competente, en el caso de que se produzca un incumplimiento de las obligaciones contractuales por cualquiera de las partes.

Otro gran problema que aporta la configuración no jerarquizada y ordenada de los contenidos de la red es el hecho de que los distintos comercios virtuales que constituyen la oferta son muy numerosos y se hallan dispersos de tal manera que al usuario le resulta muy difícil su localización cuando no dispone de referencias previas.

A pesar del gran desarrollo experimentado por los portales verticales, los buscadores y las áreas comerciales especializadas, el consumidor inexperto no puede reprimir cierto sentimiento de incertidumbre o desorientación en el momento de iniciar una sesión de Internet en la que sabe lo que quiere comprar pero no sabe dónde empezar a buscar.

A ello se une la dificultad para comparar la oferta de un comercio virtual con la de sus competidores. Aunque ello ha quedado superado con los servicios de búsqueda y comparación de ofertas que ofrecen algunos recursos, incluso gratuitos, de Internet, la mayoría de los usuarios no los conocen o no los utilizan.

De esta manera se limita la capacidad de elección del consumidor, que queda circunscrita a los comercios que ha podido localizar y visitar, y a la información que éstos suministran sobre sus productos.

En la mayoría de los casos, dicha información se extiende a la identidad de la empresa oferente y a las características de su oferta, pero todavía existe un segmento importante de comercios que no suministra la debida información al usuario que los visita, siendo la práctica más frecuente la de no especificar los pasos a seguir y los medios de contacto para efectuar una reclamación, en el caso de que se produzcan problemas en la entrega o el producto sea defectuoso.

1.2 El factor decisivo de la distancia

La distancia que separa al comprador del vendedor impide la valoración de las propiedades del producto, obstaculiza la negociación de unas cláusulas personalizadas y es inherente a cualquier relación telemática.

Esa distancia impide una presencia simultánea de las partes e influye en todas las fases de la relación, hasta el punto de merecer un tratamiento especial en la legislación sobre comercio minorista, con el objeto de aumentar la protección del consumidor ante los posibles desajustes que puedan producirse entre lo prometido por el vendedor y lo entregado, finalmente, al comprador.

En una relación presencial, el cliente puede identificar plenamente al comerciante. Conoce su identidad, su domicilio y los demás datos que le permitirán formular una reclamación en caso de incumplimiento.

La distancia en Internet supone un obstáculo para la personalización de la relación y se une a otras características técnicas de la red que permiten lanzar una oferta anónima o con una identidad falsa, con el fin de impedir el resultado positivo de una reclamación.

Aún así, la propia iniciativa empresarial que representa la oferta en Internet, ha desarrollado diversas iniciativas para contrarrestar los efectos negativos de la distancia y el fenómeno no deseado de la despersonalización y el anonimato, mediante fórmulas como el marketing "one to one", basado en la posibilidad que se ofrece al usuario de escoger los elementos que van a participar en la configuración final del producto.

1.3 Obstáculos y factores inhibidores

Las encuestas que se realizan cada año sobre el avance del comercio electrónico y la banca a través de Internet señalan, que todavía subsisten una serie de obstáculos jurídicos que el legislador debe resolver para conseguir la máxima protección del consumidor, y factores inhibidores que los usuarios deben superar, antes de que el comercio electrónico se consolide. Entre ellos destacan la desconfianza en los medios de pago, la incertidumbre respecto al tratamiento de los datos personales, y los aspectos relacionados con la seguridad. En los últimos años se han aprobado diversas normas que permiten afirmar que se ha alcanzado una situación jurídica en la que las partes que intervienen en un negocio electrónico pueden hallar una protección adecuada para sus derechos.

El objetivo de esta guía es orientar a los usuarios de Internet en sus compras por la red para que minimicen al máximo los riesgos y modifique la percepción subjetiva de algunas características de la red que pueden impedirles participar con mayor frecuencia en este tipo de transacciones.

1.4 La protección del consumidor en Internet

Tanto en el ámbito internacional como en el ámbito europeo, ha habido iniciativas para analizar los posibles riesgos para los consumidores en Internet, destacando las acciones de la Comisión Europea en este campo.

Las Administraciones Central y la Autonómica han incidido de forma repetida en el problema y han desarrollado propuestas legislativas y planes de acción para dotar de protección al consumidor.

También se ha desarrollado una labor de formación y sensibilización por parte de los organismos de consumo de ambas administraciones.

En la actualidad, el usuario dispone de un marco jurídico perfectamente aplicable al comercio electrónico y representado, principalmente, por las siguientes normas:

- Ley de Comercio Minorista.
- Ley general para la defensa de los consumidores y usuarios.
- Ley general de Publicidad.
- Directiva de contratos a distancia.
- Directiva de Comercio Electrónico.
- Ley orgánica de protección de datos de carácter personal.
- Ley de condiciones generales de contratación.
- Real Decreto sobre contratación telefónica o electrónica con condiciones generales de contratación.
- Real Decreto Ley sobre firma electrónica.
- Real Decreto de arbitraje de Consumo.
- Código Penal.
- Código Civil.

Las asociaciones de internautas se han dedicado principalmente a los problemas específicos de la red, entendida ésta como medio de comunicación y por ello se han centrado en áreas como las tarifas de acceso, la calidad del servicio de los distintos operadores del mercado de las telecomunicaciones y los estudios demográficos.

1.5 Garantías adicionales: códigos éticos

La sensibilidad de las empresas que se dedican al comercio electrónico y a la banca electrónica a través de Internet es cada vez mayor. A pesar de ello, los datos estadísticos demuestran que todavía hay mucho por hacer. Un informe de la Confederación Española de Organizaciones de Amas de Casa, Consumidores y Usuarios (CEACCU) realizado en 1999 nos da las siguientes cifras sobre el nivel de cumplimiento de las obligaciones de seguridad por parte de las empresas españolas:

- Banca: 100%
- Comercio presencial: 55%
- Comercio electrónico: 42%

Respecto al cumplimiento de las obligaciones relativas a los datos personales, el informe nos ofrece las siguientes cifras:

- Banca: 42%
- Comercio presencial: 35%
- Comercio electrónico: 15%

A pesar de que estos datos demuestran que la actividad desarrollada por las empresas en Internet no tiene todavía una madurez desde el punto de vista del respeto de las obligaciones relativas a la seguridad y a los datos personales, también es cierto que el año 1999 fue un periodo de efervescencia que originó la creación de numerosas plataformas comerciales en la red, que están todavía en fase de consolidación. Por otro lado, la autorregulación del sector está avanzando rápidamente de la mano de asociaciones como la Asociación Española de Comercio Electrónico (AECE) y la Asociación de Autocontrol de la Publicidad (AAP).

Los códigos éticos de ambas asociaciones incluyen una referencia explícita a los sistemas de obtención de datos personales a través de Internet. En el caso de AECE, la adhesión a este régimen por parte de la empresa permite utilizar un sello de garantía que informa a los usuarios del web sobre el cumplimiento de las normas contenidas en el código ético. La AECE también ofrece un apoyo a la empresa en la redacción de su política en materia de datos personales e intimidad. Este instrumento permitirá informar a los usuarios de su web sobre la naturaleza y la finalidad de los datos obtenidos a través de la misma. El objetivo básico es eliminar la desconfianza del usuario de Internet en esta materia.

Cada asociación dispone de un canal para recibir denuncias por incumplimiento del código, y un tribunal que puede retirar el sello de calidad a la empresa que incumpla dichas pautas.

2. ÁREAS ANALIZADAS

2.1 Información del comercio

Las garantías exigidas por el consumidor en las transacciones realizadas en un medio cuya principal característica es la distancia que separa ambas partes, deben extremarse justamente en lo que constituye la principal consecuencia de dicha distancia, es decir, la dificultad para conocer la verdadera identidad de nuestro interlocutor.

En este sentido, es lógico que exista un esfuerzo por parte del legislador nacional y del europeo para exigir al proveedor de un producto o servicio que utiliza un medio de comunicación, unos requisitos iniciales de información sobre los aspectos relativos a su identidad, domicilio, dirección de correo electrónico, datos mercantiles, datos profesionales y número de identificación fiscal.

Todo ello va orientado a facilitar una eventual reclamación del consumidor en el caso de que se produzca un incumplimiento contractual por parte del comercio.

2.2 Características del producto o servicio

La misma característica de la distancia que aconseja extremar las precauciones para confirmar la identidad del comercio que va a ser parte en una transacción electrónica, anima también a recomendar que se obtenga toda la información necesaria para llegar a conocer las características de un producto que el consumidor no podrá examinar hasta que llegue a su poder.

Independientemente de las garantías de devolución o desistimiento que la Ley ofrece en la venta a distancia al comprador, debe tenerse en cuenta la posibilidad de que el comercio se halle ubicado en un país donde dichas garantías no sean aplicables.

Por ello es especialmente aconsejable recopilar toda la información que sea posible sobre las propiedades técnicas y funcionales del objeto a adquirir, de manera de exista un alto nivel de coincidencia entre las expectativas del comprador y el bien finalmente entregado.

A dichas cautelas debe unirse la de prevenir el fraude basado en la entrega de cosa distinta a la prometida, o la simple no entrega del producto adquirido.

2.3 Marketing y publicidad en Internet

En Europa, la Directiva sobre comercio electrónico dispone de una sección dedicada a las comunicaciones comerciales no solicitadas en la que establece que los Estados miembros que permitan este tipo de mensajes por correo electrónico deberán exigir que este tipo de publicidad sea identificable de forma clara, inequívoca e inmediata por el destinatario. También deberán establecer medidas para asegurar que las empresas que envíen publicidad no solicitada por correo electrónico, consulten regularmente y respeten

los registros OPT-OUT en los que los usuarios que no deseen recibir este tipo de mensajes puedan inscribirse. Esta solución ha prevalecido sobre la que solicitaban algunas asociaciones de consumidores, que consistía en la prohibición de enviar mensajes publicitarios a las personas que no se hubiesen inscrito expresamente en un registro OPT-IN.

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.

La Agencia de Protección de Datos (APD) distribuye una guía para usuarios de Internet que puede obtenerse gratuitamente en <http://www.ag-protecciondatos.es>. La APD ha sancionado a una empresa que no atendió el requerimiento de un usuario que recibía mensajes solicitados, y no canceló su dirección en la base de datos.

Finalmente, cabe destacar el uso progresivo de los códigos éticos ya comentados, en los que se establecen normas sobre la utilización del correo electrónico para fines publicitarios.

En el caso de abuso, los usuarios pueden optar por requerir al remitente de los mensajes para que cese en el envío de publicidad. Si no atiende a la solicitud, puede requerir a su PSI, que seguramente habrá incluido en el contrato de servicios de Internet la obligación de no hacer spam. También puede denunciarse el abuso a las asociaciones que administran los códigos éticos que regulan el sector, o a la Agencia de Protección de datos.

2.4 Datos personales

El temor de los usuarios de Internet respecto a una posible obtención de datos relativos a sus preferencias y hábitos de consumo está plenamente justificado en un entorno tecnológico en el que existen recursos para conocer cuáles son los pasos que da un usuario de la red desde el momento en que inicia su navegación hasta que se desconecta. No obstante, el marco legislativo vigente en la actualidad en Europa y los recientes acuerdos con Estados Unidos garantizan una tutela efectiva de la intimidad en Internet. La cuestión radica en detectar y demostrar los abusos que se producen en un entorno en el que las pruebas de la infracción pueden ser tan remotas como efímeras.

Cuando un usuario visita una página web, pueden producirse una serie de operaciones informáticas que van a permitir obtener una información adicional de gran utilidad para las funciones de marketing de la empresa visitada.

Sin tener en cuenta los datos facilitados voluntariamente a través de un formulario, el usuario puede suministrar datos personales con el simple acto de visualizar la página. La obtención de dichos datos puede realizarse con distintas herramientas, entre las que destacan:

- Applets de Java.
- Javascript integrado en el código fuente HTML de la página web.

- Cookies.
- Controles ActiveX y Visual Basic.

Entre los datos obtenibles con applets de Java y Javascript, figuran los siguientes:

- Dirección de correo electrónico.
- Tipo de navegador, versión del mismo e idioma.
- Sistema operativo.
- Resolución de pantalla.
- Fuentes.
- Nombre asignado al ordenador.
- Dirección IP fija o dinámica.
- Número de páginas visitadas.
- URL de procedencia.

Además, el código fuente de la página visitada puede contener un sencillo Javascript que ordena el envío voluntario de un mensaje de correo electrónico a una dirección determinada. De esta manera, sin que el usuario lo haya autorizado, ha facilitado su dirección de correo electrónico al solicitante. Ello va a permitir a la empresa receptora de dicha dirección crear una base de datos de visitantes que han demostrado su interés por un tema específico y que, por lo tanto, pueden ser segmentados en función de sus preferencias, con el fin de efectuar posteriormente envíos de publicidad por correo electrónico.

A continuación podemos ver un ejemplo de Javascript que permite obtener la dirección de correo electrónico del visitante de una página:

```
<script LANGUAGE="JavaScript" >
<!--function sendmail() {
document.forms[0].method="post"
document.forms[0].encoding="text/plain"
document.forms[0].action="mailto:marketing@empresax.es"}!-->
</script>
```

Puede obtenerse más información sobre este apartado en el Criptonomicon: <http://www.iec.csic.es/criptonomicon>

Los controles ActiveX y los scripts y ejecutables de Visual Basic, así como cualquier otro contenido activo o programa, permiten ir más allá y obtener todo tipo de datos almacenados en el disco duro del usuario. Entre la información que puede obtenerse con estas herramientas, destaca:

- Historial de navegación.
- Datos de identificación del usuario, introducidos durante la instalación y configuración del programa navegador, o del programa correo electrónico, IRC, news, FTP, o cualquier otro.
- Direcciones de correo electrónico de otros usuarios.
- Bases de datos y agendas electrónicas.

Aunque se trata de un riesgo latente en el caso de estas herramientas, es muy poco habitual encontrar estos supuestos de obtención in consentida de datos, ya que, además de las consecuencias legales derivadas de la intromisión en la intimidad de la persona, la imagen de la empresa quedaría muy afectada. Pensemos que las pruebas de la obtención de estas herramientas son fáciles de obtener a través del código fuente de la página web, sin necesidad de ningún procedimiento especial.

Existen una serie de medidas que el usuario puede aplicar para evitar el efecto negativo de cualquier utilidad destinada a invadir su intimidad. En la propia red pueden encontrarse programas y servidores que permiten una navegación anónima a través de Internet, eliminando, sustituyendo o enmascarando los elementos identificativos del usuario, especialmente el encabezamiento de los paquetes IP transmitidos.

También existen programas que permiten administrar, filtrar o eliminar los cookies que se van a instalar o se han instalado en el disco duro del ordenador del usuario.

Existen programas rastreadores que permiten localizar direcciones de correo electrónico en los foros públicos de Internet. La arropa, el elemento común que contienen todas las direcciones, permite detectar y capturar de forma automatizada una gran cantidad de direcciones de correo electrónico, que después son introducidas en una base de datos en la que los usuarios están segmentados en función del tema debatido en el grupo de noticias o en la lista de distribución correspondiente.

Además, el IRC genera la posibilidad de que otros participantes en el chat introduzcan troyanos en el ordenador para facilitar un posterior acceso al mismo.

Las medidas de prevención consisten, en este caso, en el enmascaramiento de la dirección de correo electrónico mediante la adición de texto que provoque la devolución de los mensajes enviados a la misma. Por ejemplo: usuarioNOSPAM@dominio.es.

Finalmente, el programa navegador, el sistema operativo, el software de red local y los programas de correo electrónico, news, IRC y FTP pueden ser configurados para impedir la ejecución de scripts o contenidos que puedan comprometer la seguridad del ordenador del usuario, obteniendo información in consentida. Entre estos ajustes, podemos destacar los siguientes:

- Bloqueo o exigencia de aceptación previa para la instalación de cookies en el disco duro.
- Bloqueo de scripts y applets de Java, Visual Basic y controles ActiveX.
- Bloqueo de la ejecución remota de aplicaciones.
- Filtro de contenidos activos.
- Bloqueo del envío automático de correo electrónico.
- Alerta en el caso de reenvío de formularios a otras direcciones.
- Alerta en el caso de pasar de entornos seguros a entornos inseguros.
- Alerta en el caso de ejecución de contenidos activos.
- Alerta en el caso de certificados caducados o emitidos por entidades no reconocidas.

2.5 Condiciones generales de contratación

El uno de marzo del 2000 entró en vigor el Real Decreto que regula la contratación electrónica con condiciones generales de contratación. Se trata de un importante avance para el comercio electrónico en nuestro país, ya que en él se establecen las garantías que deben ofrecerse a los consumidores y usuarios en la contratación basada en la simple adhesión a unas cláusulas previamente redactadas, de forma unilateral y sin posibilidad de negociación, por el comercio oferente.

Este es el sistema utilizado por la práctica totalidad de los comercios en Internet y por cualquier otra actividad comercial que vaya dirigida a un elevado número de destinatarios. La Ley de Condiciones Generales de Contratación establece la posibilidad de que la aceptación de las cláusulas que regulan la transacción electrónica se efectúe sin presencia física de las partes intervinientes y sin necesidad de firma convencional. Este Real Decreto desarrolla las condiciones en que dicha modalidad de contratación puede tener lugar.

- Deber de información previa

El comercio oferente debe facilitar al consumidor, de modo veraz, eficaz y completo, información sobre todas y cada una de las cláusulas del contrato, y remitirle, por cualquier medio adecuado a los medios utilizados en Internet para establecer la comunicación a distancia: página web y correo electrónico. Esta información deberá facilitarse con carácter previo a la celebración del contrato, y como mínimo, en los tres días naturales anteriores a la misma.

- Confirmación documental

Una vez celebrado el contrato, el comercio deberá enviar al consumidor de forma inmediata y, como máximo en el momento de la entrega de la cosa, o inicio de la prestación del servicio, justificación por escrito de la contratación efectuada, en la que constarán los términos de la misma. El usuario puede escoger cualquier otro soporte duradero como un disquete informático o el disco duro donde almacena los mensajes de correo electrónico recibidos.

- Derecho de resolución

El consumidor dispondrá de un plazo de siete días hábiles, a partir de la recepción del producto, para resolver el contrato sin incurrir en penalización ni gastos alguno, incluidos los correspondientes a la devolución del bien.

- Carga de la prueba

Corresponde al comercio oferente la prueba de la existencia y contenido de la información previa de las cláusulas del contrato celebrado a través de Internet, de la entrega al consumidor de las condiciones generales, de la justificación documental de la contratación efectuada, de la renuncia expresa al derecho de resolución, así como de la correspondencia entre la información, entrega y justificación documental y el momento de sus respectivos envíos.

Para ello, el comercio puede utilizar cualquier medio de prueba admitido en derecho, como el sistema de certificación de condiciones generales de contratación descrito en <http://www.lortad.com/cgcaudit.com> aunque el Real Decreto comentado da

especial significación a los documentos electrónicos y telemáticos que cumplan los principios de autenticación, integridad y constancia de las fechas de emisión y recepción. Para ello, deberá utilizarse una firma electrónica avanzada que atribuya a los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita, de acuerdo con la normativa reguladora de la firma electrónica. El documento electrónico deberá llevar también consignada la fecha y hora de su emisión y recepción.

Cabe decir que es evidente que la aplicación de esta norma contribuirá al aumento de la confianza del consumidor en esta modalidad de contratación, pero también hay que reconocer que aumenta los obstáculos para constituir un comercio en Internet, especialmente en el periodo transitorio que medie hasta la consolidación del uso de la firma.

En otro orden de cosas, se han detectado dificultades en los contratos que se aceptan mediante un click en el botón de aceptar de un formulario, las cuales se resumen a continuación:

1. Existe el riesgo de que el usuario pulse el botón de aceptación de forma accidental, por error o sin ser consciente de las consecuencias de dicha acción.
2. Para el usuario supone una carga adicional leer un contrato en pantalla, mientras está conectado, pagando unas tarifas que dependen justamente de la duración de la llamada. Las prisas, la ansiedad del comprador compulsivo, el descuido o la indiferencia hacen que, en muchos casos, se pulse el botón "aceptar" sin leer las condiciones generales de contratación. Es un fenómeno al que se ha dado en llamar "síndrome de Dilbert" porque recuerda una tira cómica de este personaje, en la que Dilbert se quejaba de haber instalado un programa de Microsoft y de haber aceptado, sin darse cuenta, ser el toallero de la mansión de Bill Gates. Tampoco podía acudir a su abogado, porque éste había instalado otro programa de Microsoft y ahora era el chófer de Bill Gates.
3. Es difícil demostrar la asociación directa entre el consentimiento prestado por el usuario y el contenido de las cláusulas.
4. Los constantes cambios en los contenidos de una página web y en la propia política comercial de la empresa oferente, dificultan la prueba sobre la versión de las condiciones generales que aceptó un usuario concreto en el momento de la compra.
5. Aumenta la posibilidad de que surja una picaresca que se aproveche de estas circunstancias para justificar la falta de pago. Empiezan a ser frecuentes las anulaciones de pedidos basadas en la aceptación accidental o en el desconocimiento de las obligaciones asumidas.

A pesar de ello, el nivel de incidencias ocasionado por estos motivos en la actualidad no llega al uno por ciento de las transacciones realizadas, salvo en el caso de productos que se distribuyen en formato digital, y que se obtienen directamente a través de la red, en los que el nivel de incidencias puede llegar a superar el cinco por ciento.

La primera decisión judicial relativa a la validez de los contratos celebrados a través de Internet la dictó un Juzgado de California en el caso *Hotmail contra Van\$ Money Pie Inc.*

Hotmail había demandado a una empresa que utilizaba su servicio de correo electrónico para enviar publicidad no solicitada (spam) y basaba su reclamación en un incumplimiento de las condiciones generales de contratación que había aceptado on line, al contratar su cuenta de correo electrónico en Hotmail. En este caso, el tribunal californiano entendió que había suficiente base documental para apreciar la validez del contrato y fundamentó su decisión en las condiciones generales de contratación aceptadas al pulsar un botón del formulario electrónico.

Recordemos que en España, el Reglamento ya comentado, por el que se desarrolla el artículo cinco de la Ley sobre Condiciones Generales de Contratación exige que, con carácter previo a la celebración del contrato se facilite al usuario, de modo veraz, eficaz y completo, información sobre todas y cada una de las cláusulas del contrato. También se establece la obligación de enviar al usuario justificación por escrito de la contratación efectuada, en la que consten todos los términos de la misma.

2.6 Medios de pago

La seguridad en las transacciones sigue siendo uno de los principales factores inhibidores para el comercio electrónico. Según el estudio de la Asociación Española de Comercio Electrónico (AECE) correspondiente al ejercicio de 1999, la percepción del usuario de Internet respecto a los sistemas de pago utilizados en las transacciones electrónicas es, todavía, de desconfianza. Un 23,17 por ciento de los encuestados declararon que el principal obstáculo para decidirse a comprar a través de la red era la falta de confianza en los medios de pago, mientras que 19 por ciento se refirió al miedo a facilitar datos personales en Internet. Otros obstáculos que se mencionaron fueron la desconfianza de los usuarios en que el pedido cursado y pagado sea realmente entregado (10,39%) y la desconfianza en el propio proveedor (7,3%).

Sin embargo, una vez que el usuario ya se ha iniciado en la compra a través de Internet, el medio preferido es justamente la tarjeta de crédito, debido a la comodidad y rapidez que proporciona.

El nivel real de incidencias es mínimo. Según el Instituto Gallup, sólo el 9% de los usuarios encuestados en 1999 manifestaron haber tenido alguna vez un problema de seguridad en Internet.

Todo ello, unido al hecho de que la Ley permite al usuario anular cualquier cargo indebido que se haya producido en la cuenta de su tarjeta de crédito, confirma que la sensación de inseguridad del usuario de Internet obedece a la percepción subjetiva que tiene de una materia que no conoce. La valoración del riesgo, en suma, lo sitúa en una cota que está por encima de la realidad.

Actualmente, el empresario prefiere asumir el riesgo de la falta de autenticación antes que perder al cliente ocasional que encuentra su web, navegando por Internet, y decide comprar de forma espontánea.

Hasta ahora, el protocolo SSL ha cumplido perfectamente esa función, ya que permite realizar una compra inmediata, sin que la propia transacción se convierta en un obstáculo, y con un umbral de seguridad aceptable para el comprador.

Sin embargo, los textos que hasta ahora se han dedicado a describir o regular la seguridad en las operaciones electrónicas de contenido económico, han prestado mayor atención a la seguridad de los servidores y redes implicadas en la transacción electrónica que en la seguridad física de la llamada última milla, es decir, el ordenador del usuario final, y la conexión que le une a su proveedor de acceso a Internet. Citando algunos ejemplos, la Directiva sobre firmas electrónicas y el RDL de firma electrónica se basan en los principios de autenticidad, confidencialidad, integridad y eficacia jurídica aplicados a los documentos validados con la firma electrónica avanzada. Los tres libros que describían el funcionamiento de la especificación SET dedicaban diversos apartados a los mecanismos de seguridad que se aplican en las operaciones necesarias para llegar a consumir una transacción electrónica.

Pero tras una primera lectura de esos textos, se percibe que las normas están orientadas principalmente a los proveedores de servicios de certificación y a los comercios que constituyen la oferta en Internet. No existen obligaciones específicas para el comprador como parte que interviene en la transacción, que debe aplicar unas medidas básicas de seguridad para estar a la altura del esfuerzo que han hecho los demás operadores del mercado, y el propio legislador, para garantizar un umbral mínimo de seguridad jurídica.

Es evidente que la transacción debe ser el centro de atención de cualquier especificación o protocolo de seguridad, pero los usuarios no deben olvidar que también tendrán que establecer las correspondientes cautelas en la conservación de los elementos estáticos que intervienen en la operación o que son el resultado de la misma. Nos referimos al PIN, a los certificados, las claves privadas, y los demás elementos de seguridad cuya custodia corresponde al usuario, y en otro nivel, a los documentos electrónicos que quedan almacenados en su ordenador tras las fases de validación y consumación de la transacción.

Ello hace recomendable establecer un régimen contractual que obligue al usuario a cumplir unas normas de seguridad específicas para el entorno de su ordenador y para el uso y conservación de los elementos de seguridad cuyo uso exclusivo le ha sido confiado por la entidad de certificación.

Una de las cuestiones que deben abordarse en el contrato es la presunción de que, salvo prueba en contrario, es el titular del certificado, y no otro, el que ha participado en la transacción. Es decir, el usuario asume la responsabilidad de la custodia de la clave privada y por ello, las consecuencias de una conducta negligente en su conservación.

En los primeros textos de la propuesta de Directiva sobre firma electrónica existía una referencia expresa a dicha presunción, que ha quedado integrada en el artículo 5 del texto final, al establecer que los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel.

Las obligaciones del usuario con respecto a la custodia de los elementos de seguridad deben extenderse a todos los dispositivos utilizados para realizar una compra a través de Internet. Si el certificado ha sido instalado en el navegador de su PC, debe mantener unas medidas de seguridad esenciales que impidan el acceso a las claves que permitirían suplantar su identidad. En el caso de que el certificado se halle en una tarjeta inteligente, ésta debe

permanecer siempre en poder del usuario, evitando dejarla insertada en la ranura del lector de tarjetas. También deben evitarse los sistemas de memorización automática de la contraseña o PIN necesario para la fase final de la transacción.

Finalmente, cuando no se opere con el ordenador propio, debe evitarse la utilización de sistemas que no merezcan confianza, en los que pueda existir algún mecanismo de explotación de la memoria caché o cualquier otro dispositivo que permita extraer, copiar o memorizar alguno de los elementos de seguridad utilizados por el usuario.

2.7 Fiscalidad

Entre las distintas iniciativas legislativas que la Comisión Europea está lanzando en materia de comercio electrónico, destaca el proyecto para modificar la sexta Directiva IVA (77/388/CEE) aprobado el 7 de junio que pretende modificar el régimen del Impuesto sobre el Valor Añadido aplicable a las prestaciones de servicios y sujetos pasivos, en relación con los bienes digitalizados (*software*, música, servicios de *web-hosting*, *web-design* y similar etc.) comercializados de forma onerosa a través de Internet.

En el texto presentado por la Comisión se comprueba el interés del legislador europeo en impedir que se escapen del ámbito de la fiscalidad de la Comunidad las operaciones relacionadas con ciertas prestaciones de servicios realizadas por vía electrónica (prestaciones de servicios on-line) en favor de terceros países como Estados Unidos con implantación del comercio electrónico mucho más avanzada y consolidada.

Básicamente la modificación pretende que los servicios *on-line* (realizados por vía electrónica) se sometan a imposición en la Unión Europea en el caso en que se destinen al consumo interno con independencia de quien sea el destinatario (sujeto pasivo del Impuesto o particular), mientras que no serían gravados en caso de que el servicio prestado por un empresario o profesional comunitario fuese objeto de consumo fuera de la Unión.

Por otro lado también se pretende delimitar la naturaleza de las transmisiones de bienes digitalizados vía Internet, ya que la definición de las prestaciones de servicios como aquellas que no puedan calificarse de entrega de bienes está dando lugar a muchas dudas e interpretaciones en muchos casos más que cuestionables.

Debido a que las normas existentes no permiten garantizar que los servicios prestados por vía electrónica puedan, en todos los casos, ser “exportados” exentos de derechos ni que haya una base jurídica suficiente para poder aplicar el IVA a los servicios prestados a consumidores privados de la UE por operadores extranjeros se produce un falseamiento de la competencia al situar a los proveedores de servicios de la UE en una posición competitiva desfavorable con relación a los proveedores de servicios de países terceros. Por esta razón el proyecto establece el gravamen en el lugar de destino o establecimiento del usuario. Ello se materializa en que:

- Se propone eximir del IVA a las prestaciones por vía electrónica a clientes establecidos fuera de la UE.
- Los prestadores de servicios establecidos en terceros países (no UE) que vendan a consumidores establecidos en la Comunidad deberán aplicar los impuestos sobre las mismas bases que un operador de la UE cuando efectúen transacciones comerciales en la Comunidad.

Para ello se prevé establecer un *único registro*, así como un límite máximo de registro que permita excluir a operadores muy pequeños de países terceros o a los que sólo realicen prestaciones muy ocasionales en la Comunidad.

No obstante, quedan exentos de dichas obligaciones los operadores que presten servicios en la UE por un valor anual agregado inferior a los 100.000 euros.

La propuesta cubre también el tratamiento fiscal de los servicios de radiodifusión y teledifusión prestados mediante suscripción o pago por conexión ya que las disposiciones fiscales existentes discriminan a las empresas europeas y se traducen en una ventaja de precio importante en favor de los operadores de terceros países.

Asimismo, la Comisión se propone examinar los tipos impositivos que se establecen para las entregas de bienes y las prestaciones de servicios a efectos de evitar el problema respecto de las posibilidades de aplicar tipos diferentes a bienes y servicios claramente similares.

Por último señalar que el redactado de la propuesta contempla la necesidad de elaborar herramientas directamente coercitivas a las que puedan recurrir las administraciones fiscales en aras de garantizar el cumplimiento de la normativa y crear el clima de confianza necesario para que el comercio electrónico pueda hacerse realidad. La Comisión animará a todas las autoridades nacionales de aplicación que intervengan en el control del cumplimiento de las obligaciones por empresas de comercio electrónico a cooperar e intercambiar información con el resto de administraciones.

2.8 Responsabilidad civil

Los supuestos de responsabilidad civil derivada de operaciones de comercio electrónico, tendrán su origen, en la mayoría de los casos, en aspectos relacionados con la calidad de los productos o servicios suministrados. La aplicación de la Ley General para la Defensa de Consumidores y Usuarios y, en consecuencia supone la posible nulidad de las cláusulas de exoneración de responsabilidad. No obstante, este tipo de cláusulas será plenamente válido cuando el comprador integre el producto adquirido en su sistema productivo o de prestación de servicios.

Para poder efectuar una reclamación de daños y perjuicios es importante conservar copia de las páginas web en las que se incluían las características de la oferta y toda la documentación correspondiente al producto y a la transacción.

2.9 Resolución de controversias

En el caso de incumplimiento contractual de cualquiera de las partes, puede existir una voluntad de reclamación en el afectado que, posiblemente, se verá frustrada por una serie de dificultades relacionadas de forma directa o indirecta con el medio en el que se realiza la transacción electrónica, y entre las cuales destacan las siguientes:

- La falta de especificación, en algunas ocasiones, de un conducto por el que el consumidor pueda remitir sus reclamaciones al comercio.
- El desconocimiento de la identidad real y el domicilio del vendedor.

- La incertidumbre relativa a la jurisdicción aplicable y la jurisdicción competente.
- El contraste que se produce entre la rapidez con la que se realiza la transacción y la lentitud de cualquier proceso de reclamación judicial.
- La inexistencia de un proceso ágil, sencillo y económico para reclamar por una operación de comercio electrónico fallida.
- La falta de especialización de comercio electrónico, Internet y redes telemáticas de los funcionarios de la Administración Justicia.
- La ineficacia de la sentencia de un tribunal español en países donde no existe la posibilidad de ejecutarla.

Estas razones han hecho que la Comisión Europea haya propuesto, en repetidas ocasiones, la creación de tribunales arbitrales rápidos y especializados en esta materia.

Finalmente, el Arbitraje de Consumo constituye una alternativa válida y eficaz para este tipo de controversias, en los casos en que resulta aplicable.

2.10 Fraudes y delitos en Internet

La Federal Trade Commission norteamericana, entidad a la que corresponde la tutela de los derechos del consumidor, ha elaborado recientemente (Octubre del 2000) una lista de los fraudes más habituales en Internet.

Las denuncias presentadas por los consumidores en los últimos años evidencian que los supuestos de fraude más frecuentes en el comercio electrónico, son los siguientes:

- Productos milagro.
- Periodos de prueba que se prorrogan y facturan sin el consentimiento expreso del consumidor.
- Desvíos de comunicaciones a líneas 906 que generan cargos no esperados.
- Ventas piramidales.
- Fraudes en subastas on line.
- Penalizaciones desproporcionadas por la cancelación anticipada de servicios a largo plazo.
- Cargos solicitados en tarjetas de crédito.
- Fraude en la contratación de viajes y vacaciones.
- Fraude en ofertas de negocios y oportunidades de inversión.
- Planes de inversión que no cumplen los compromisos de rentabilidad prometida.

En el apartado de delitos, uno de los riesgos más altos para el usuario de Internet es la destrucción de datos provocada por la entrada de un virus informático en su ordenador. Este riesgo puede extenderse a la participación del perjudicado en la propia actividad de difusión del virus.

El análisis de la responsabilidad derivada de la difusión de un virus merece especial atención en estos momentos en que el uso intensivo de redes telemáticas permite un mayor alcance de sus efectos. Prueba de ello la tenemos en la reciente difusión por correo electrónico del virus "I love you".

Para analizar los diferentes supuestos que generan responsabilidad, debemos tener en cuenta los canales de difusión que contribuyen a potenciar el efecto pirámide en el que los virus basan su efectividad. En todos ellos es aplicable el régimen de responsabilidad extracontractual establecido en el artículo 1902 del Código Civil, que obliga a reparar los daños a quien, por acción u omisión, causa un perjuicio a otro, interviniendo culpa o negligencia.

- Creación

La mera creación de un virus puede obedecer a una intención distinta a la puesta en circulación: participar en un concurso, competir con otros virus, crear armas de guerra electrónica, etc.

- Puesta en circulación

Es difícil obtener una identificación plena del responsable de la puesta en circulación del virus. Aunque en el caso de redes telemáticas es posible encontrar rastros de la primera aparición del virus, es posible alterar esa información.

En cualquier caso, la responsabilidad de la persona que inicia la cadena de efectos nocivos de un virus, planificando la difusión intencionada del mismo a través de un medio de transmisión está clara, pues el daño es perfectamente previsible y seguro.

- Introducción intencionada en un sistema específico

Por su tipificación como delito de daños, los actos de sabotaje informático pueden generar responsabilidad civil y penal. Pueden tener su origen en personas del interior de la empresa que por un motivo como la ruptura de la relación laboral, deciden causar un daño, o en personas del exterior de la empresa, que acceden al sistema informático por medios telemáticos. En ambos casos se cumplen los requisitos para reclamar una indemnización.

El artículo 264.2 del Código Penal castiga con la pena de prisión de uno a tres años 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.

- Difusión de virus entre usuarios

La difusión involuntaria de un virus entre usuarios de sistemas informáticos puede tener dos niveles:

- La difusión debida a una conducta negligente.
- La difusión de virus no catalogados.

La diligencia debida en el tratamiento de la información obliga a realizar copias de seguridad y a instalar sistemas de detección de virus. En el caso de archivos que se envían

a otros usuarios, la ausencia de control previo puede ser calificado como negligente, puesto que el riesgo de destrucción de datos se está traspasando a otros colectivos y ello podía haberse evitado de una manera sencilla y económica. Pero también puede alegarse que el usuario receptor del archivo afectado podría haber evitado el daño pasando el correspondiente anti-virus, a lo que cabe replicar que este trámite se obvió por tratarse de un remitente que ofrecía confianza.

En cualquier caso, el Reglamento de seguridad de la LORTAD establece la obligación de realizar copias de seguridad, al menos una vez a la semana, cuando el sistema informático contiene datos personales de tipo básico.

Cuando el virus que afecta al archivo transmitido no está incluido en el catálogo de virus del programa de detección utilizado, por tratarse de una clase de reciente aparición, la conducta diligente del usuario debería ser suficiente para enervar la responsabilidad. Para ello, el usuario deberá mantener actualizado el programa anti-virus con los archivos suministrados periódicamente por el fabricante.

Un detalle paradójico lo constituye el artículo 96.3 del Texto Refundido de la Ley de Propiedad Intelectual, al establecer la exclusión de los virus de las creaciones protegidas por el derecho de autor. El objetivo de este precepto es facilitar las actividades de análisis necesarias para la creación de un antivirus, pero resulta innecesario por la sencilla razón de que el creador de un virus no acostumbra a reclamar la titularidad del mismo de forma pública.

Además del delito de daños que puede representar la difusión de un virus, el usuario de Internet está expuesto a otros delitos que pueden afectarle de forma directa o indirecta. Entre ellos, destacan los siguientes:

Acceso no autorizado.- La protección de un ordenador conectado a Internet frente a accesos no autorizados desde la red es un desafío constante, ya que exige mantener el sistema actualizado con los últimos parches del sistema operativo y las herramientas para detectar caballos de Troya, fisuras de seguridad, etc. A pesar de ello, si un ataque tiene éxito y se produce un acceso no autorizado al sistema, una acción inmediata permitirá, en la mayoría de los casos, conocer el posible origen y la ruta seguida por el atacante, siempre que la colaboración de los propietarios de los servidores implicados facilite la investigación. Aunque el acceso no autorizado no provoque daños en los datos del usuario, el hecho de introducirse en un sistema, además de constituir una vulneración de la intimidad, exige la alteración previa de los mecanismos de seguridad, el uso no autorizado de los terminales que facilitan el acceso y la interceptación de los elementos dinámicos y estáticos que permiten que el ordenador pueda participar como terminal en una comunicación telemática. Todas estas actividades están previstas en los artículos 197, 256 y 264 del Código Penal.

Saturación intencionada del servidor.- Se trata de los ataques que sufrieron los principales portales americanos el pasado mes de febrero, consistente en el envío masivo de órdenes de consulta con la dirección de respuesta errónea, con el fin de bloquear el servidor. Las acciones tendentes a inutilizar datos, documentos o programas informáticos, de forma temporal o definitiva, constituyen un delito de daños, previsto en el artículo 264 del Código Penal. En este caso, el perjuicio para el usuario es la imposibilidad de acceder a la página web atacada.

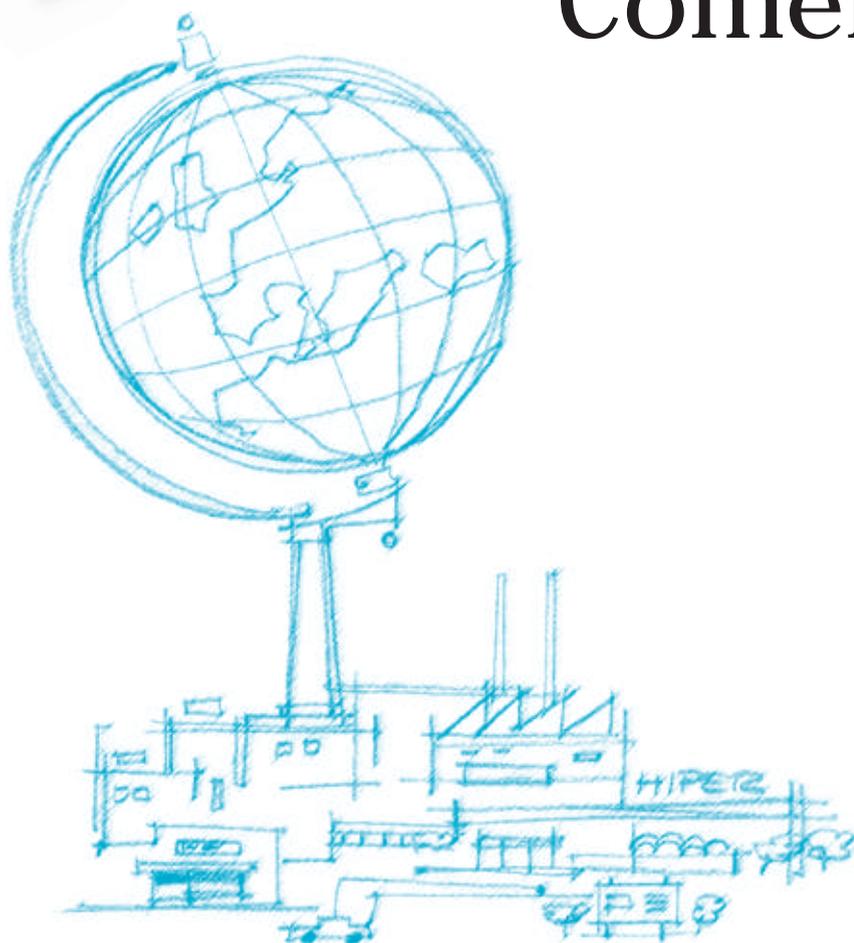
Captura de datos de tarjetas de crédito.- Es el supuesto que más preocupa al consumidor, y figura entre los principales factores inhibidores del comercio electrónico. Aunque la trascendencia real es mínima, ya que la normativa sobre venta a distancia permite al titular de la tarjeta anular de forma inmediata y sin necesidad de prueba los cargos indebidos, la percepción subjetiva del usuario sigue siendo de desconfianza en el medio. La utilización de "sniffers", es decir, programas que permiten interceptar el tráfico de paquetes IP que genera una transacción electrónica, está tipificado como delito en el artículo 197 del Código Penal.

Estafas electrónicas.- En este caso, el artículo 248.2 del Código Penal castiga la actividad realizada con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante con la que se consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. La jurisprudencia anterior al Código Penal de 1995 había considerado que no existía estafa en los supuestos en los que se engañaba a un sistema informático y no a una persona. La actual configuración del tipo penal permite perseguir los fraudes cometidos en las transacciones de comercio electrónico.

3/1

área

Información del Comercio



3.1.1

Indicación de los datos identificadores del comercio

ÁREA ANALIZADA

Aunque el consumidor o usuario que contrata a través de Internet puede permanecer en el anonimato cuando la naturaleza y el precio del producto o servicio contratado lo permiten, el comercio está obligado a identificarse de forma inequívoca a sus clientes.

Las operaciones de consumo a través de Internet se basan en un contacto a distancia que se inicia, en la mayoría de los casos, mediante la visualización de la página web del comercio por parte del cliente potencial. La falta de mención de la identidad del comercio en su web puede impedir al usuario tener conocimiento del nivel de garantía o seriedad que merece esa oferta comercial y puede dificultar el acceso posterior a los servicios de posventa, información y reclamaciones.

ACTIVIDAD PREVENTIVA

- Buscar en la página principal los datos del oferente.
- Buscar los datos en el formulario de pedido.
- Buscar una dirección de correo electrónico.
- Buscar un formulario de consultas o contacto con el oferente.
- Imprimir la página en la que constan los datos del oferente.
- Guardar los datos del oferente junto a los comprobantes de la transacción.

ACCIONES A REALIZAR EN CASO DE NO LOCALIZAR LOS DATOS DEL OFERENTE

- En el caso de que exista un formulario de contacto, solicitar los datos.
- En el caso de que se facilite una dirección de correo electrónico, solicitar los datos.
- En caso extremo puede consultarse la titularidad del dominio en el registro.
- Si es posible obtener los datos del oferente, es aconsejable no realizar la compra.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista:

.- Artículo 40.

.- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>

.- Artículo 4.

ÁREA ANALIZADA

Es muy importante determinar, con carácter previo a la transacción, la nacionalidad del comercio que está ofreciendo sus productos o servicios a través de Internet. En algunas ocasiones la localización geográfica del comercio no es fácil de determinar, y se trata de un asunto importante, ya que puede incidir en las siguientes cuestiones:

- Plazos de entrega.
- Gastos de transporte.
- Calidad del producto.
- Impuestos aplicables.
- Procedimiento a seguir para las devoluciones.
- Costes derivados de la devolución.
- Legislación aplicable.
- Jurisdicción competente.
-

ACTIVIDAD PREVENTIVA

- Buscar en la página principal la localización geográfica del oferente.
- Buscar la sede social en el formulario de pedido.
- Buscar una dirección de correo electrónico.
- Buscar un formulario de consultas o contacto con el oferente.

ACCIONES A REALIZAR EN CASO DE NO AVERIGUAR LA LOCALIZACIÓN

- En el caso de que exista un formulario de contacto, solicitar los datos postales.
- En el caso de que se facilite una dirección de correo electrónico, solicitar los datos postales.
- En caso extremo puede consultarse la titularidad del dominio en el registro.
- Si es posible determinar la localización geográfica del oferente, es aconsejable no realizar la compra.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista:

.- Artículo 40.

.- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>

.- Artículo 4.

ÁREA ANALIZADA

El principal problema de la contratación a distancia es la imposibilidad de determinar que la persona que contrata con nosotros es realmente quien dice ser y no se trata de una suplantación. En Internet, el problema se agrava por la ausencia de sellos, firmas manuscritas y elementos de identificación convencionales.

Además, la facilidad actual para obtener un nombre de dominio .COM por parte de cualquier persona abre la posibilidad de que un defraudador registre el dominio de una empresa conocida y suplante su identidad.

En cualquier caso, el comercio se halla en la misma situación que el usuario, ya que, al no poder identificarlo como titular del medio de pago utilizado, se arriesga a que se produzca una anulación del cargo efectuado en la tarjeta de crédito.

Aunque la solución se halla en el uso de certificados electrónicos y en la aplicación de la firma electrónica, existen todavía muchos comercios y usuarios que no han accedido a esta tecnología, por lo que, en caso de duda, conviene recurrir a las técnicas tradicionales de identificación.

ACTIVIDAD PREVENTIVA

- Buscar en la página principal los datos del oferente.
- Buscar los datos en el formulario de pedido.
- Buscar una dirección de correo electrónico.
- Buscar un formulario de consultas o contacto con el oferente.
- Imprimir la página en la que constan los datos del oferente.
- Visualizar el certificado del servidor.

ACCIONES A REALIZAR EN CASO DE SOSPECHA

- Cotejar los datos obtenidos con los de la empresa presuntamente suplantada.
- Confirmar la identidad con los datos del proveedor telemático del comercio.
- En caso extremo puede consultarse la titularidad del dominio en el registro.
- Si no es posible despejar la incertidumbre sobre la identidad del comercio, es aconsejable no realizar la compra.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista:

.- Artículo 40.

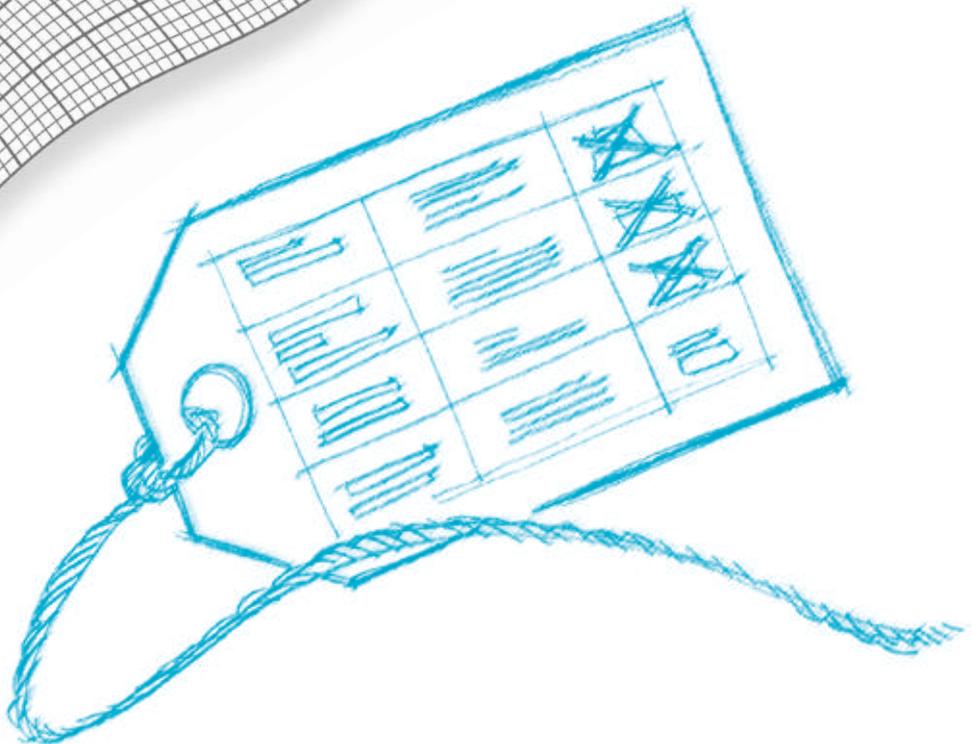
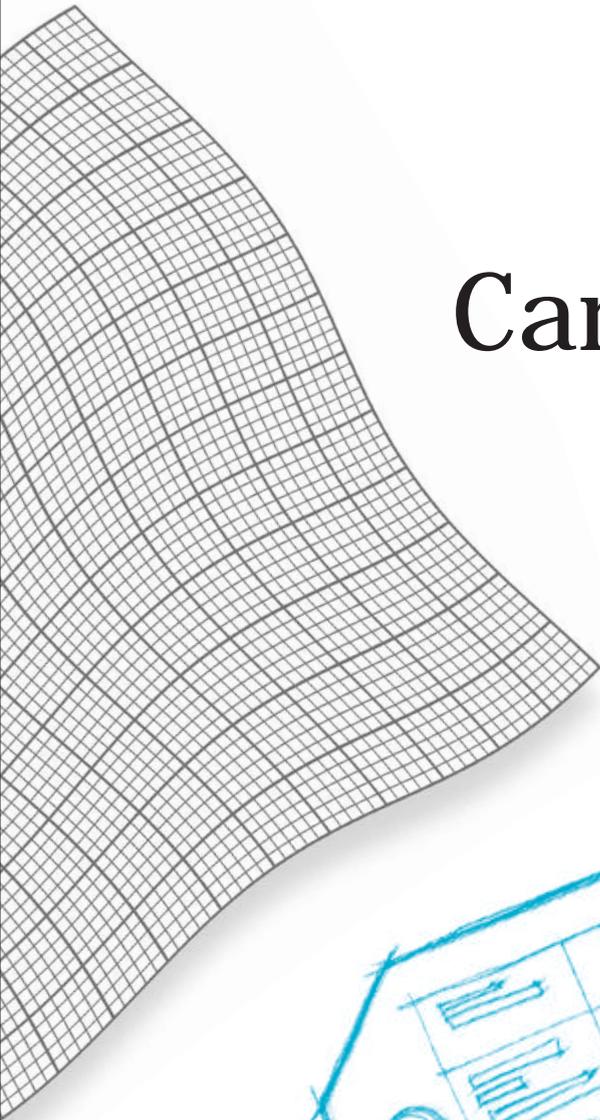
.- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>

.- Artículo 4.

3/2

área

Características del Producto o Servicio



3.2.1

Indicación de las características del producto

ÁREA ANALIZADA

Con el fin de evitar errores en la interpretación de las propiedades del producto o servicio ofrecido a través de Internet, es importante que todas sus características, y en especial el precio, queden correctamente indicadas en la página web. Al tratarse de un medio de contratación a distancia, las características del producto no pueden ser apreciadas de forma directa por el consumidor, por lo que debe realizarse un esfuerzo para reproducir fielmente lo que va a constituir el objeto de la operación.

Entre los datos que deben figurar en la oferta, destacan los siguientes:

- Precio.
- Forma de pago.
- Características técnicas.
- Requisitos necesarios para la utilización.
- Garantías aplicables.
- Régimen de reclamaciones.

ACTIVIDAD PREVENTIVA

Antes de adquirir el producto, compruebe que dispone de toda la información necesaria para decidir sobre la conveniencia de dicha adquisición.

ACCIONES A REALIZAR

En caso de no disponer de toda la información necesaria para decidir sobre la conveniencia de adquirir el producto, solicítela al oferente.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>
- .- Artículo 7.2.
- .- Artículo 7.3.

ÁREA ANALIZADA

El carácter internacional de la red y la posibilidad de crear páginas web de forma anónima permite ser aprovechado para suministrar productos de origen ilícito a través de Internet. Estos productos son fáciles de distinguir por su bajo precio o por el carácter gratuito de la entrega.

El hecho de que el comprador no haya participado en la actividad de obtención y distribución del producto ilícito no implica que esté exento de responsabilidad, por lo que deberán adoptarse las medidas oportunas para evitar este tipo de riesgos.

La posibilidad de adquirir productos ilegales no está limitada a los objetos o sustancias que se entregan de forma física. También pueden ser ilícitos los archivos informáticos que se descargan a través de la propia red.

Entre los primeros estarían los productos robados o falsificados, y todos aquellos cuyo tráfico esté prohibido (Por ejemplo: armas, sustancias estupefacientes, etc.).

Entre los segundos figurarían especialmente los archivos que contienen obras de propiedad intelectual cuya reproducción se ha efectuado sin la autorización del titular de los derechos de explotación. (Por ejemplo: programas de ordenador, fotografías, gráficos, informes, música en formato MP3, MP4, etc.).

ACTIVIDAD PREVENTIVA

- Compruebe el precio del producto ofrecido en otras sedes web de suministradores legalmente establecidos, que ofrezcan garantías de licitud.
- Exija siempre la factura o un documento acreditativo de la compra, en el que figuren todos los datos del vendedor.
- En el caso de programas de ordenador que se descargan a través de la red, si el suministrador no es el propio titular de los derechos de explotación, solicite que acredite que está autorizado para distribuir el programa.
- En el caso de música en formato MP3, MP4 o similares, exija al suministrador que acredite que el fichero ha sido reproducido con autorización del titular del Copyright.
- En el caso de productos gratuitos, extreme las precauciones.

ACCIONES A REALIZAR

En el caso de detectar la oferta de un producto ilegal en Internet, cuyo suministrador se halle presumiblemente en España, debe denunciarlo a través de las siguientes vías:

1. Enviar un mensaje al propietario del servidor en el que se encuentra alojada la página web que contiene la oferta del producto ilícito, con el fin de que proceda a su retirada.
2. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es

Productos ilegales

La denuncia de un delito, además de una obligación, es un acto de solidaridad, que evitará que otras personas resulten perjudicadas por la misma infracción.

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 301.

ÁREA ANALIZADA

Existen numerosas páginas web en Internet que ofrecen productos farmacéuticos no autorizados en España o que necesitan receta médica. Dichas ofertas provienen generalmente de países en los que no existe un control sobre la venta de productos farmacéuticos o donde la venta de determinadas sustancias está autorizada.

La adquisición y consumo de productos farmacéuticos por canales distintos a los autorizados puede suponer un grave peligro para la salud.

ACTIVIDAD PREVENTIVA

Por regla general, no es aconsejable adquirir productos farmacéuticos a través de Internet, ya que no existe la posibilidad de comprobar la fecha de caducidad del mismo ni garantizar que el medio de transporte utilizado no altere las propiedades del producto.

Por otra parte, la mayoría de estos productos sólo pueden ser vendidos en farmacias y, algunos de ellos, previa exhibición de la correspondiente receta médica.

ACCIONES A REALIZAR

- Compruebe en el Boletín Oficial del Estado la lista de productos autorizados para su venta en España.
- Por regla general, no adquiera productos farmacéuticos a través de Internet.

LEGISLACIÓN APLICABLE

- .- Leyes de distintos organismos oficiales sobre la venta de productos farmacéuticos en España.
- .- Recomendaciones de la Organización Mundial de la Salud en materia de venta de productos farmacéuticos.

ÁREA ANALIZADA

La sensación de ausencia de control que a veces genera Internet hace que, en ocasiones, se exageren las cualidades de un producto. Algunas veces, el producto ha sido diseñado para ofrecerlo como algo excepcional, capaz de resolver problemas que ningún otro producto ha conseguido con anterioridad. Son los llamados productos milagro y acostumbran a ser ofrecidos desde países con escaso control sobre la publicidad engañosa.

ACTIVIDAD PREVENTIVA

- Compruebe el precio del producto ofrecido en otras sedes web de suministradores.
- Contraste las cualidades del producto con otros de la misma naturaleza.
- Verifique la identidad del oferente.
- Busque referencias de otros usuarios.
- Compruebe si existen referencias del producto en alguna asociación de defensa de los consumidores y usuarios.
- Compruebe si existen referencias del producto en los organismos de consumo de la Administración Central, Autonómica o Local.

ACCIONES A REALIZAR

- Solicite una descripción por escrito de las propiedades del producto.
- Solicite garantías respecto a la calidad del producto.
- En caso de incertidumbre sobre la calidad del producto, no lo adquiera.

LEGISLACIÓN APLICABLE

- .- Ley 34/1988, de 11 de noviembre, General de Publicidad:
- .- Artículo 4.
- .- Artículo 5.

ÁREA ANALIZADA

Mientras que las entidades financieras españolas están sujetas a una regulación específica y a una supervisión del Banco de España, los productos financieros extranjeros ofrecidos a través de Internet pueden provenir de entidades no sometidas a ningún tipo de control. En especial, las entidades radicadas en paraísos fiscales pueden ofrecer una elevada rentabilidad a cambio de un mayor riesgo.

Por otro lado, la Agencia Tributaria dispone de un sistema informático que permite cruzar los datos originados por las transferencias de fondos a entidades financieras radicadas en el extranjero. La finalidad de este control es conseguir mayor transparencia en las inversiones realizadas a través de Internet y disponer de estadísticas que permitan detectar las áreas de riesgo, haciendo más efectiva la lucha contra el fraude.

ACTIVIDAD PREVENTIVA

- Antes de establecer contacto con una entidad que ofrece productos a través de Internet, compruebe desde qué país está operando.
- Solicite asesoramiento a su Banco o Caja antes de utilizar los servicios de una entidad financiera radicada en el extranjero, especialmente si se halla en un paraíso fiscal.
- Compruebe los límites y requisitos formales vigentes en ese momento para realizar una inversión en el extranjero.
- Analice las obligaciones fiscales aplicables a los intereses resultantes de una inversión en el extranjero.
- Analice detenidamente las condiciones de rescate de la inversión, las garantías ofrecidas y los trámites de repatriación del capital.

ACCIONES A REALIZAR

- Identificación clara de la entidad financiera.
- Revisión de las condiciones generales de contratación por un experto.
- Solicitud de un justificante de la transacción en un soporte duradero.

LEGISLACIÓN APLICABLE

.- Legislación relativa a inversiones en el extranjero.

.- Legislación fiscal aplicable a la contratación de productos financieros en el extranjero.

3/3

área

Marketing y Publicidad en Internet



3.3.1

Obstáculos para la navegación

ÁREA ANALIZADA

Algunas páginas web incluyen en su código fuente una función que consiste en bloquear el comando BACK del navegador, impidiendo la posibilidad de volver hacia atrás en el historial de páginas visitadas. De esta manera se consigue que el tiempo de permanencia en dicha página sea mayor, aumentando la eficacia de la publicidad contenida en la misma. Esta función, al igual que otras que persiguen la misma finalidad, no infringen la Ley, aunque entorpecen la navegación del usuario y pueden ir en contra de la etiqueta de la red o de los códigos éticos establecidos por las asociaciones de anunciantes.

ACTIVIDAD PREVENTIVA

No existen medidas específicas para prevenir los efectos de los obstáculos a la navegación. Éstos surgen al visitar las páginas web de aquellos anunciantes que han decidido forzar la permanencia del usuario y la única prevención puede ser la referencia previa de otros usuarios que hayan visitado este tipo de páginas y adviertan de su existencia, así como la experiencia del propio usuario.

Existen páginas web que relacionan los nombres y direcciones de los anunciantes que incluyen este tipo de técnicas.

En cualquier caso, la escasa trascendencia de estos obstáculos, y la facilidad con la que pueden ser sorteados, hace desaconsejable invertir demasiado tiempo en prevenirlos. Finalmente, la apreciación de las molestias provocadas por estos obstáculos es muy subjetiva, por lo que el deseo de prevenirlos varía en cada usuario.

ACCIONES A REALIZAR

- En el caso de bloqueo de la función BACK (Ir hacia atrás) pulsar el botón del navegador que permite visualizar las páginas visitadas con anterioridad y seleccionar cualquiera de ellas.
- En el caso de iniciarse la apertura de una nueva ventana o sesión del navegador cuyo contenido tarde en visualizarse y obstaculice la visión de los contenidos de la página visitada, puede cerrarse la ventana antes de que finalice la descarga.
- En el caso de que el obstáculo sea realmente molesto o tenga efectos de excesiva duración, puede visitarse la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>
- .- Artículo 12.- Publicidad en la world wide web.

ÁREA ANALIZADA

Al navegar por Internet, en ocasiones se visitan páginas que contienen un tipo de publicidad que no se limita a exhibir un simple mensaje publicitario estático mediante un banner, sino que generan una acción que obliga al usuario a prestar atención sobre un contenido también publicitario que aparece sin que haya sido solicitado, y que consume recursos del ordenador o de la red, obstaculizando de forma momentánea la navegación y la visualización de los contenidos que en realidad estaba buscando el usuario. Es la llamada publicidad intrusiva. Es difícil determinar qué acciones publicitarias son intrusivas, ya que ello depende de la duración, de los recursos que consumen y del criterio subjetivo del usuario, que puede sentirse más o menos molesto en función del tiempo que pueda invertir en su visualización y de las características de su ordenador, navegador, módem, ancho de banda contratado, etc. Acostumbran a ponerse como ejemplos de este tipo de publicidad las "pop-up window", los "interstitials" y los "superstitials". Los dos últimos contienen elementos multimedia.

ACTIVIDAD PREVENTIVA

No existen medidas específicas para prevenir la publicidad intrusiva. La única prevención puede ser la referencia previa de otros usuarios que hayan visitado este tipo de páginas y adviertan de su existencia, así como la experiencia del propio usuario.

Existen páginas web que relacionan los nombres y direcciones de los anunciantes que incluyen este tipo de técnicas.

También pueden seleccionarse las opciones avanzadas del navegador que permiten impedir la ejecución de contenidos activos sin la autorización del usuario.

ACCIONES A REALIZAR

- En el caso de iniciarse la apertura de una nueva ventana o sesión del navegador cuyo contenido tarde en visualizarse y obstaculice la visión de los contenidos de la página visitada, puede cerrarse la ventana antes de que finalice la descarga.
- En el caso de iniciarse la visualización de un interstitial o superstitial que tarde en visualizarse y obstaculice la visión de los contenidos de la página visitada, puede cerrarse la ventana antes de que finalice la descarga.
- En el caso de que la publicidad sea realmente molesta o tenga efectos de excesiva duración, puede visitarse la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.

LEGISLACIÓN APLICABLE

.- Directiva de contratos a distancia.

.- Ley 34/1988, de 11 de noviembre, General de Publicidad.

.- Código Ético sobre publicidad en Internet de la Asociación de Autocontrol de la Publicidad. <http://www.aap.es>

ÁREA ANALIZADA

Existen programas de ordenador que permiten capturar direcciones de correo electrónico en páginas web, grupos de noticias, chats y otros foros públicos.

La finalidad de esta captura es crear bases de datos que permitan el envío de forma masiva de mensajes publicitarios. En ocasiones, también son comercializadas.

Estas bases de datos permiten segmentar a los destinatarios en función de las preferencias que han demostrado al encontrarse en foros temáticos dedicados a intereses o aficiones comunes de los usuarios que forman parte de los mismos. Aunque el hecho de indicar la dirección de correo electrónico en un foro público puede ser interpretado como una autorización tácita para el envío de mensajes, el usuario puede considerar el uso de su dirección, asociada a una afición concreta, como una invasión de su intimidad.

El tratamiento automatizado de direcciones de correo electrónico es analizado en el apartado de datos personales.

ACTIVIDAD PREVENTIVA

- Limite el uso de direcciones de correo electrónico en foros públicos
- En el caso de participar en foros públicos, puede enmascarar la dirección de correo electrónico con caracteres adicionales que impidan su uso si no se retiran de forma manual. Por ejemplo "usuarioQUITAR@psi.es"

ACCIONES A REALIZAR

- En caso de detectar la existencia de una base de datos que contiene su dirección de correo electrónico en contra de su voluntad, puede solicitar la cancelación del dato al responsable del fichero.
- En caso de no conocer la identidad del responsable del fichero, puede dirigirse al remitente de cualquier mensaje publicitario recibido sin previo consentimiento, solicitando la cancelación del dato.
- En el caso de uso reiterado e incontestado de su dirección de correo electrónico para el envío de mensajes publicitarios, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos en <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

- .- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal <http://www.onnet.es/03002016.htm>
- .- Código Etico AAP - <http://www.aap.es>
- .- Código Etico AECE - <http://www.aece.org>
- .- Recomendaciones de la APD - <http://www.agenciaprotecciondatos.org>

ÁREA ANALIZADA

El envío masivo de mensajes publicitarios a través de correo electrónico (spam) es una opción atractiva por su bajo coste económico, pero puede suponer un alto coste de imagen para la empresa anunciante por ir en contra de la etiqueta de la red. Los usuarios de Internet han luchado desde el inicio de la red contra la utilización del correo electrónico para el envío de publicidad no solicitada.

En la práctica, la mayoría de las empresas recurren a sistemas que gozan de mayor aceptación por parte de los usuarios (banners, buscadores, portales, prensa escrita...) y en los casos en que se utiliza el correo electrónico se acostumbra a hacer con prudencia, pidiendo disculpas por la utilización de este medio y facilitando una dirección de correo electrónico donde se puede solicitar la baja en la lista de distribución o base de datos de destinatarios.

ACTIVIDAD PREVENTIVA

- Limite el uso de direcciones de correo electrónico en foros públicos.
- En el caso de participar en foros públicos, puede enmascarar la dirección de correo electrónico con caracteres adicionales que impidan su uso si no se retiran de forma manual. Por ejemplo "usuarioQUITAR@psi.es"
- También puede utilizar filtros "anti-spam"

ACCIONES A REALIZAR EN EL CASO DE RECIBIR PUBLICIDAD NO SOLICITADA

- Compruebe si en el mensaje se indica el procedimiento que debe seguir el receptor del mensaje para solicitar que no se remita más publicidad a dicho destinatario.
- En caso positivo, si no desea recibir más publicidad, siga el procedimiento indicado en el mensaje para solicitar la cancelación de sus datos.
- En caso negativo, si no desea recibir más publicidad, envíe un mensaje a la dirección del remitente del mensaje solicitando la cancelación de los datos.
- Si recibe más mensajes publicitarios del mismo remitente transcurridos diez días desde el envío del mensaje de cancelación, puede optar por:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

.- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: <http://www.onnet.es/03002016.htm> : artículo 16.

ÁREA ANALIZADA

Internet da una sensación de impunidad o de ausencia de control que puede hacer que alguna empresa se vea tentada a exagerar las características o propiedades de un producto o servicio. Cuando la publicidad es susceptible de generar un error a sus destinatarios que sea capaz de afectar a su comportamiento económico, dicha publicidad puede ser calificada como engañosa.

ACTIVIDAD PREVENTIVA

- Contraste las cualidades del producto con otros de la misma naturaleza.
- Verifique la identidad del oferente.
- Busque referencias de otros usuarios.
- Compruebe si existen referencias del producto en alguna asociación de defensa de los consumidores y usuarios.
- Compruebe si existen referencias del producto en los organismos de consumo de la Administración Central, Autonómica o Local.

ACCIONES A REALIZAR

- Solicite una descripción por escrito de las propiedades del producto.
- Solicite garantías respecto a la calidad del producto.
- En caso de incertidumbre sobre la calidad del producto, no lo adquiera.
- En caso de comprobar un supuesto de publicidad engañosa, puede ponerlo en conocimiento de la Asociación de Autocontrol de la Publicidad, a través de la página web <http://www.aap.es>

LEGISLACIÓN APLICABLE

- .- Ley 34/1988, de 11 de noviembre, General de Publicidad.
- .- Artículo 4.
- .- Artículo 5.

ÁREA ANALIZADA

Las mismas circunstancias que rodean la publicidad engañosa hacen que en algunas ocasiones, el mensaje de publicidad tenga un contenido ofensivo. Pueden llegar a ser ofensivos aquellos contenidos que atenten contra la dignidad de la persona, o sean discriminatorios (por razón de nacionalidad, raza, sexo, orientación sexual, convicciones religiosas o políticas).

ACTIVIDAD PREVENTIVA

La publicidad ofensiva no puede ser objeto de prevención en destino, sino en origen. No existen medidas específicas para que un usuario pueda prevenir la visualización de mensajes publicitarios ofensivos. Éstos surgen al visitar las páginas web de aquellos anunciantes que han decidido optar por una forma agresiva de comunicación y la única prevención puede ser la referencia previa de otros usuarios que hayan visitado este tipo de páginas y advierta de su existencia, así como la experiencia del propio usuario.

Existen páginas web que relacionan los nombres y direcciones de los anunciantes que incluyen este tipo de publicidad.

Finalmente, la apreciación del carácter ofensivo de un mensaje publicitario es muy subjetiva, por lo que el deseo de prevenirlas varía en cada usuario.

ACCIONES A REALIZAR

- En caso de comprobar un supuesto de publicidad ofensiva, puede ponerlo en conocimiento de la Asociación de Autocontrol de la Publicidad, a través de la página web <http://www.aap.es>

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>
- .- Artículo 3.4.

ÁREA ANALIZADA

El carácter personal y el bajo coste de las comunicaciones a través de Internet permite enviar un gran número de mensajes publicitarios a destinatarios de correo electrónico, grupos de noticias o páginas web, bajo la forma de un relato, una experiencia personal, una noticia, etc., de manera que la inducción al consumo se produce de forma velada, como testimonio de otro usuario y no como un anuncio remitido por el anunciante. La publicidad encubierta resulta por lo tanto mucho más efectiva, aunque puede generar confusión en un usuario inexperto, que acabe creyendo la veracidad del testimonio aportado en el mensaje publicitario.

ACTIVIDAD PREVENTIVA

La publicidad encubierta siempre persigue el objetivo de inducir al destinatario al consumo y se reconoce por la mención una marca específica y una página web en la que se puede encontrar más información del producto o servicio anunciado de forma encubierta.

ACCIONES A REALIZAR

- En caso de comprobar un supuesto de publicidad encubierta que considere grave o abusivo, puede ponerlo en conocimiento de la Asociación de Autocontrol de la Publicidad, a través de la página web <http://www.aap.es>

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

.- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>

.- Artículo 5.

ÁREA ANALIZADA

El medio más utilizado para localizar información sobre productos y servicios en Internet son los llamados buscadores, que actúan como inmensos índices en los que se agrupan y clasifican por categorías de contenidos los diferentes recursos que existen en la red. Entre estos buscadores destacan Altavista, Yahoo, Lycos, Olé, Telépolis y un largo etcétera.

Cuando introducimos una palabra con el fin de que el motor de búsqueda nos muestre las páginas web que están relacionadas con ese tema, el buscador nos presenta los resultados divididos en varias páginas. En cada página aparecen entre 10 y 25 direcciones que cumplen los requisitos establecidos en las instrucciones y acotaciones que se han dado al buscador. El problema estriba en que, según las estadísticas, el usuario medio de un buscador no acostumbra a pasar de la tercera página, y las probabilidades de que se llegue a hacer click en una dirección y visitar el web se concentra en las tres primeras URL's que aparecen en la lista.

No es de extrañar que el objetivo de todas las empresas dedicadas al comercio electrónico consista en figurar entre esas codiciadas primeras posiciones, que van a garantizar la afluencia de visitantes interesados en el tipo de producto que ofrecen en sus páginas web. Para lograr este objetivo, existen varios métodos, con una trascendencia jurídica distinta, como veremos a continuación.

El primero de ellos es el alquiler exclusivo de palabras, que consiste en un contrato publicitario con la empresa que gestiona el buscador, mediante el que se garantiza que en todas las búsquedas relacionadas con ese tema, aparecerá el web del anunciante en el primer lugar de la lista. Un posible uso desleal de este recurso sería alquilar en exclusiva las marcas de las empresas competidoras.

Cuestión distinta es la el contrato publicitario mediante el que la empresa que gestiona el buscador se obliga a presentar un banner o anuncio gráfico enlazado al web del anunciante cada vez que un usuario introduce alguna de las palabras alquiladas en exclusiva en la base de datos del buscador.

Otro método consiste en el uso de metatags. Los metatags o metanames son palabras que se introducen en el código fuente HTML de una página web con distintos propósitos, entre los cuales destaca el de indicar a los buscadores las palabras clave que representan los temas tratados en dicho web. Los metatags están ocultos en el código fuente y no se visualizan en pantalla durante la navegación.

A veces se introducen como metatag sinónimos o palabras que guardan relación con los contenidos del web, pero en otros casos, se incluyen los términos estadísticamente más utilizados en los buscadores, con el fin de aumentar la afluencia de visitantes. El uso de metatags puede constituir un acto de competencia desleal cuando se utilizan marcas notorias o nombres de productos de empresas competidoras para atraer a la propia página web a los usuarios de un buscador que introduzcan dichas palabras como criterio de búsqueda. Además de un uso no autorizado de la marca, puede existir un aprovechamiento ilícito de la reputación de una empresa o de un producto. También puede apreciarse un engaño al usuario que acude a la página web pensando que va a encontrar información sobre un artículo determinado y encuentra otro distinto.

Actos de confusión en buscadores

ACTIVIDAD PREVENTIVA

Cuando utilice un navegador, compruebe que las páginas que cumplen el criterio de búsqueda introducido se refieren realmente al producto que está buscando.

ACCIONES A REALIZAR

En el caso de detectar un uso inapropiado de una marca, con el consiguiente riesgo de confusión para los usuarios de dicho producto, puede remitir un mensaje de advertencia al fabricante.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Ley 3/1991, de 10 de enero, de Competencia Desleal:
- .- Artículo 6.
- .- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es>
- .- Artículo 8.3.

ÁREA ANALIZADA

Los lenguajes HTML y JavaScript con los que se desarrollan las páginas web permiten dividir la pantalla del navegador en diferentes ventanas o FRAMES, cuyo contenido puede estar formado por otras páginas HTML del propio web o de otros webs.

Cuando se visualiza la página de destino dentro de un "frame", el navegador sigue indicando la URL o dirección de la página de origen, de manera que, tras un periodo de navegación, el usuario puede llegar a confundir los contenidos de la página de destino con los de la página de origen. Cuando esta confusión se busca de manera intencionada, puede producirse un supuesto de competencia desleal, ya que el usuario puede creer erróneamente que los contenidos visualizados han sido desarrollados por el titular de la página web de origen.

ACTIVIDAD PREVENTIVA

- Cuando visite una página con "frames" compruebe que los contenidos visualizados dentro del frame, que van a ayudarle a decidir si va a realizar o no la compra, corresponden efectivamente a la empresa cuyo web está visitando.
- Para ello existen varias opciones, por ejemplo, comprobar la coincidencia entre el dominio principal del web (<http://www.XXXXX.es>) que aparece en la parte superior del navegador, y los dominios a los que apuntan los links o enlaces hipertextuales de la página principal.
- Otra posibilidad consiste en comprobar si existe una versión del web sin frames, o en eliminar los frames haciendo "click" en el link con el botón derecho del mouse, y eligiendo la opción: "abrir destino en una ventana nueva"
- Si no está seguro de que la descripción del producto que está visualizando corresponde a la empresa que lo está ofreciendo, tenga precaución antes de realizar la compra.

ACCIONES A REALIZAR

- En caso de comprobar un supuesto de confusión con "frames" en una página web, puede ponerlo en conocimiento de la Asociación de Autocontrol de la Publicidad, a través de la página web <http://www.aap.es>

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

.- Ley 3/1991, de 10 de enero, de Competencia Desleal:

.- Artículo 6. Actos de confusión.

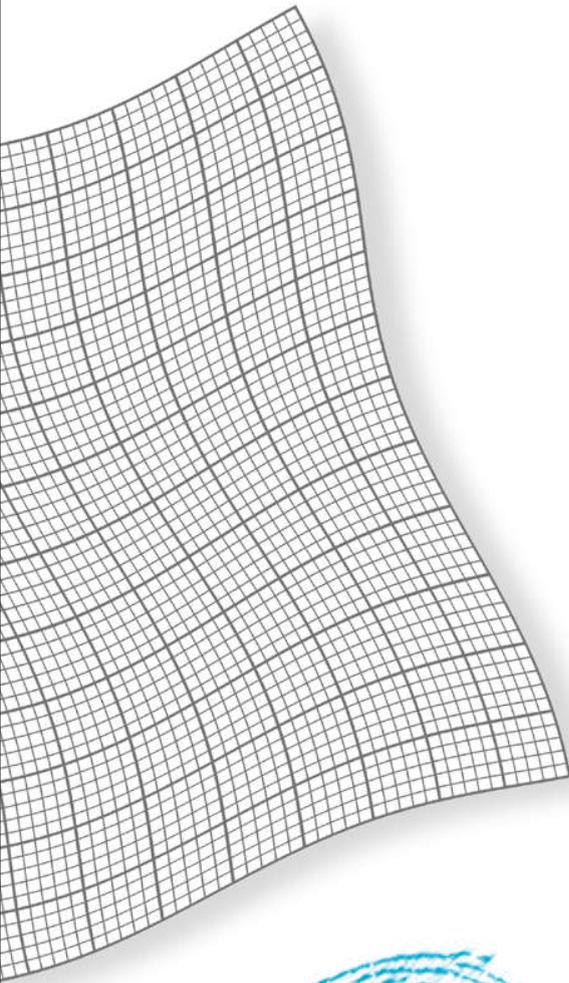
.- Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad: <http://www.aap.es> –

.- Artículo 8.2.

3/4

área

Datos Personales



ÁREA ANALIZADA

Cuando un usuario cumplimenta un formulario en papel puede tener ciertas dudas sobre el tratamiento informático posterior de sus datos personales, pero cuando se cumplimenta un formulario a través de Internet, no cabe ninguna duda respecto a su tratamiento automatizado, ya que el propio usuario está introduciendo sus datos personales en un sistema informático. Los campos de los formularios se hallan enlazados con los campos de las bases de datos instaladas en el servidor del comercio. De esta manera, puede obtenerse una integración completa entre la recogida de datos que se produce en el entorno gráfico que sirve de interfaz con el usuario y la gestión posterior de dicha información en la base de datos.

Pese a ello, muchos de los formularios de recogida de datos que podemos encontrar en Internet, adolecen de una ausencia total de referencias a la Ley orgánica de protección de datos de carácter personal en forma de cláusulas de consentimiento por parte del usuario respecto al tratamiento automatizado de los datos personales introducidos, así como de una información sobre la posibilidad de modificar o incluso cancelar los registros referentes a su persona.

La firma original del afectado será necesaria en el caso de recogida de datos referentes a la salud. Por ejemplo, la contratación a través de Internet de seguros de vida o invalidez, la solicitud de ingreso en mutuas médicas, y demás servicios relacionados con la salud, exigirá el posterior envío del documento original en papel, con la firma del usuario.

ACTIVIDAD PREVENTIVA

- Cuando cumplimente un formulario en el que se soliciten sus datos personales, compruebe que se cumplen los requisitos establecidos en la Ley orgánica de protección de datos de carácter personal.
- En especial, compruebe la existencia de un texto mediante el que usted pueda otorgar su consentimiento al tratamiento de los datos personales facilitados.
- Compruebe también que el formulario de recogida de datos utiliza un servidor seguro, que garantice la confidencialidad de los datos personales suministrados.

ACCIONES A REALIZAR

- En el caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar

Consentimiento del usuario

una queja sobre la actividad de una empresa que contravenga dicho código ético.

3. Visitar la página web de la Agencia de Protección de Datos en <http://www.ag-protecciondatos.es> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

- .- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. <http://www.onnet.es/03002016.htm>
- .- Artículo 6. Consentimiento del afectado.
- .- Recomendaciones a usuarios de Internet de la Agencia de Protección de Datos. <http://www.agenciaprotecciondatos.org>

ÁREA ANALIZADA

El usuario de Internet que tenga conocimiento de que sus datos personales han sido incluidos en una base de datos, tiene derecho a solicitar el acceso a los mismos, con el fin de comprobar si son correctos y solicitar su rectificación, o cancelarlos, en el caso de que no desee que sean objeto de tratamiento.

ACTIVIDAD PREVENTIVA

- En el caso de tener conocimiento de que sus datos personales están incluidos en una base de datos, compruebe cuál es el procedimiento para ejercitar los derechos de acceso, rectificación y cancelación.

ACCIONES A REALIZAR

- En el caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos: <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

- .- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. <http://www.onnet.es/03002016.htm>
- .- Artículo 15: Derecho de acceso.

ÁREA ANALIZADA

Los datos personales de un usuario de Internet pueden ser cedidos a terceros sin su consentimiento. El objeto de dicha cesión puede ser el obtener una contrapartida económica a cambio de la posibilidad de enviar mensajes publicitarios adecuados a las preferencias de los usuarios pertenecientes a dicha base de datos.

ACTIVIDAD PREVENTIVA

- Analice el régimen contractual aplicable a la relación establecida con sus suministradores en Internet, con el fin de comprobar si se ha incluido una autorización para ceder los datos a terceros.

ACCIONES A REALIZAR

- En caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos en <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

- .- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. <http://www.onnet.es/03002016.htm>
- .- Artículo 27: Comunicación de la cesión de datos.

ÁREA ANALIZADA

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 ha cambiado con el tiempo, y ha llegado a ser un 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.

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.

Contenido

Los cookies pueden contener datos personales o cualquier otro tipo de información relacionada con el interface cliente-servidor. La Ley de protección de datos personales 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.

Asociación de los datos a una persona identificada o identificable

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 dio 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.

Función

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 el interface 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

Cookies

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 Ley de protección de datos personales, ya que la información se obtiene sin el consentimiento del usuario.

Consentimiento del usuario

También debe analizarse el nivel de consentimiento del usuario. 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 in 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.

ACTIVIDAD PREVENTIVA

- Configure su ordenador para que le advierta cada vez que un fichero cookie intente instalarse en su ordenador.
- Existen programas específicos para impedir la entrada de cookies.
- Al entrar por primera vez en una página web, compruebe si dispone de una política en materia de protección de datos personales, y si en ella se menciona el uso de cookies.

ACCIONES A REALIZAR

- Para comprobar si tiene cookies en su ordenador, una de las posibilidades es ver el contenido del subdirectorio COOKIES del directorio WINDOWS. Generalmente son ficheros TXT cuya denominación está formada por el nombre del ordenador o del usuario del navegador, una arroba y el nombre de dominio del servidor visitado en el que se ha instalado el cookie.
- Antes de decidir si desea borrarlos o no, compruebe que no estén realizando alguna función previamente autorizada por usted: personalización de una página, control de acceso a una base de datos, etc.
- Existen programas específicos para limpiar un ordenador de cookies.

LEGISLACIÓN APLICABLE

.- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. <http://www.onnet.es/03002016.htm>

.- Artículo 6: Consentimiento del afectado.

ÁREA ANALIZADA

Navegar por Internet significa dejar un rastro voluntario o involuntario sobre la actividad desarrollada. A través de formularios o mediante otras técnicas, el usuario va mostrando cuáles son sus preferencias y sus hábitos de consumo. Estos datos pueden ser utilizados para establecer perfiles y segmentar una base de datos en función de las distintas categorías de usuarios, de manera que las posteriores ofertas o mensajes publicitarios se adecuen al perfil de cada destinatario.

ACTIVIDAD PREVENTIVA

- Sea consciente de que la actividad desarrollada en Internet puede ser analizada por las empresas por las personas físicas o jurídicas con las que entre en contacto.
- Utilice navegadores que permitan bloquear la entrada de cookies.
- Si lo considera necesario, active las medidas de seguridad y confidencialidad que incorpora su navegador.
- Si lo considera necesario, utilice sistemas de navegación anónima.
- Cuando cumplimente un formulario en el que se soliciten sus datos personales, compruebe que se cumplen los requisitos establecidos en la Ley orgánica de protección de datos de carácter personal.
- En especial, compruebe la existencia de un texto mediante el que usted pueda otorgar su consentimiento al tratamiento de los datos personales facilitados.
- Compruebe también que el formulario de recogida de datos utiliza un servidor seguro, que garantice la confidencialidad de los datos personales suministrados.

ACCIONES A REALIZAR

- En el caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos en <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE

- .- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. <http://www.onnet.es/03002016.htm>
- .- Artículo 4. Calidad de los datos.
- .- Artículo 5. Derecho de información en la recogida de datos.
- .- Artículo 6. Consentimiento del afectado.
- .- Recomendaciones a usuarios de Internet de la Agencia de Protección de Datos. <http://www.agenciaprotecciondatos.org>

ÁREA ANALIZADA

De forma progresiva, cada vez más empresas están informando a los usuarios que visitan su página web sobre cuál es su política respecto a los datos personales que recaban, incluyendo una mención a la finalidad de la recogida de datos, el tipo de datos que solicitan, los métodos empleados (formularios, cookies, etc.) y las medidas de seguridad establecidas. Por otro lado, la Asociación Española de Comercio Electrónico, AECE, dispone de un código ético al que pueden adherirse las empresas que se comprometan a respetar los principios de protección de datos personales. Las empresas adheridas a este código se reconocen por un logo especial que insertan en la página principal de su web.

ACTIVIDAD PREVENTIVA

- Compruebe si la página principal del comercio visitado incluye una referencia o un link a la política de la empresa en materia de datos personales.
- Compruebe si la página principal del comercio visitado incluye el logo de la AECE.
- Visite la página web de la AECE (<http://www.aece.org>) para obtener más información sobre este tema.

ACCIONES A REALIZAR

- En el caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos en <http://www.agenciaprotecciondatos.org> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Código ético de la AECE. <http://www.aece.org>
- .- Artículo 19: *objeto*.
- .- Artículo 20: *obtención*
- .- Artículo 23: *Presentación de Reclamaciones*.

ÁREA ANALIZADA

Existen muchos comercios en Internet cuyos productos van dirigidos al público infantil. Los menores pueden tener dificultades para entender la naturaleza de la información que se les solicita o las finalidades a las que se puede destinar la información obtenida. Los anunciantes que operan a través de Internet dirigidos principalmente a menores se han comprometido, a través de iniciativas como el Código Ético de la AECE, a animar a los padres a participar y supervisar las experiencias on-line de sus hijos.

ACTIVIDAD PREVENTIVA

- Establezca las cautelas que considere oportunas respecto al uso de Internet por parte de los miembros de su familia que sean menores de edad.
- Compruebe si la página principal del comercio visitado incluye una referencia o un link a la política de la empresa en materia de menores.
- Compruebe si la página principal del comercio visitado incluye el logo de la AECE.
- Visite la página web de la AECE (<http://www.aece.org>) para obtener más información sobre este tema.

ACCIONES A REALIZAR

- En el caso de detectar una infracción de la Ley orgánica de protección de datos de carácter personal, puede optar por cualquiera de las siguientes vías:
 1. Visitar la página web de la Asociación de Autocontrol de la Publicidad en <http://www.aap.es> en la que puede consultarse el código ético para la publicidad en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad publicitaria de un anunciante que contravenga dicho código ético.
 2. Visitar la página web de la Asociación Española de Comercio Electrónico en <http://www.aece.org> en la que puede consultarse el código ético para la protección de los datos personales en Internet, y se explican los pasos a seguir para enviar una queja sobre la actividad de una empresa que contravenga dicho código ético.
 3. Visitar la página web de la Agencia de Protección de Datos en <http://www.agenciaprotecciondatos.org.es> donde encontrará unas recomendaciones específicas para usuarios de Internet y un formulario para la presentación de denuncias.

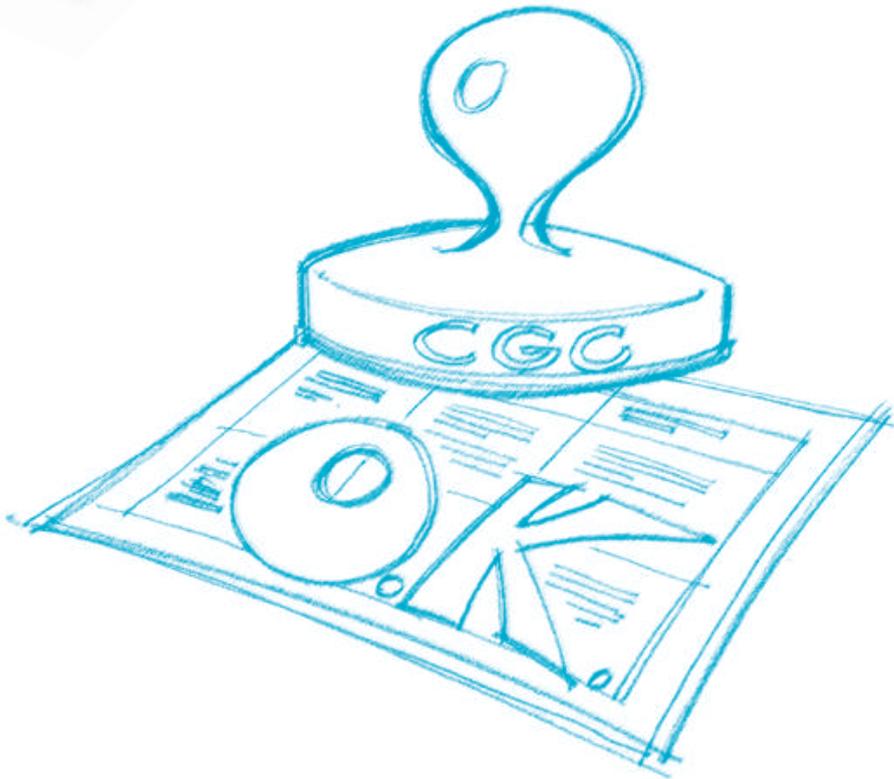
LEGISLACIÓN APLICABLE Y CÓDIGOS ÉTICOS

- .- Código ético de la AECE. E. <http://www.aece.org>
- .- Artículo 13: *objeto de la comunicación con los menores de edad.*
- .- Artículo 14: *ámbito de aplicación de los principios referidos a menores.*
- .- Artículo 15: *intervención de los padres en el tratamiento de los datos de sus hijos menores.*
- .- Artículo 16: *uso de los datos de menores.*
- .- Artículo 17: *Información del uso de los datos relativos a menores.*

3/5

área

Condiciones Generales de Contratación



ÁREA ANALIZADA

El comercio electrónico a través de Internet se basa en un sistema de contratación a distancia dirigido a una pluralidad de personas con las que no se tiene un contacto individualizado. Ello hace que la modalidad de contratación utilizada sea la de establecer unas condiciones generales a las que los usuarios se adhieren en el momento de la adquisición de un producto o la contratación de un servicio.

La validez jurídica de este sistema está condicionada al conocimiento previo, por parte del usuario, del contenido de las cláusulas que forman las condiciones generales de contratación.

ACTIVIDAD PREVENTIVA

- Compruebe que la oferta incluida en el web contempla los siguientes aspectos:
 - a) Identidad del proveedor.
 - b) Características especiales del producto.
 - c) Precio y, en su caso, debidamente separados, los gastos de transporte.
 - d) Forma de pago y modalidades de entrega o de ejecución.
 - e) Plazo de validez de la oferta.
- Antes de adquirir el producto, compruebe que dispone de toda la información necesaria para decidir sobre la conveniencia de dicha adquisición
- Antes de adquirir el producto, compruebe que dispone de las condiciones generales de contratación que regirán en la adquisición del mismo.

ACCIONES A REALIZAR

- En el caso de no disponer de las condiciones generales de contratación que regirán la adquisición del producto, solicítelas al comercio con carácter previo a la adquisición del producto o a la contratación del servicio.

LEGISLACIÓN APLICABLE

- .- Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13-4-1998, de condiciones generales de la contratación.
- .- Artículo 2. Deber de información previa.
- .- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia:
- .- Artículo 4: Información previa.

ÁREA ANALIZADA

El comercio electrónico a través de Internet está basado en la contratación a distancia con una pluralidad de personas físicas o jurídicas. Ello impide entrar en una negociación personalizada, caso por caso, debido a la dificultad para establecer un diálogo en tiempo real y al elevado número de transacciones que se producen.

A pesar de que la oferta tiende a adaptarse a las preferencias del comprador, siguiendo las directrices del marketing "one to one", las cláusulas del contrato obedecen a un esquema de contratación masiva, que se basa en la adhesión a unas condiciones generales establecidas de forma unilateral por el vendedor, que el comprador acepta en el momento en que hace "click" en un icono o botón gráfico para enviar los datos del formulario que acaba de cumplimentar.

La fórmula habitual es presentar 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 contracts" o "point-and-click agreements", que basan su validez en la muestra de consentimiento que supone el acto de pulsar el botón de aceptación por parte del usuario y tienen gran similitud con las licencias utilizadas en la comercialización de software empaquetado, que se aceptan mediante un "click" durante el proceso de instalación del programa.

ACTIVIDAD PREVENTIVA

- Establezca las cautelas que considere oportunas respecto al uso de Internet por parte Procure no pulsar el botón de aceptación de forma accidental.
- Sea consciente de que el acto de pulsar el botón significa aceptar las condiciones generales de contratación.
- Si no dispone de tiempo para leer las condiciones generales de contratación, imprimalas y difiera la aceptación final hasta el momento en que las haya leído.

ACCIONES A REALIZAR

- Imprima el formulario de pedido y aceptación de las condiciones generales de contratación, con todos los datos introducidos, antes de hacer "click" en el botón de aceptación.

LEGISLACIÓN APLICABLE

- .- Ley 7/1998, de 13 de abril, de Condiciones Generales de Contratación.
- .- Artículo 5. Requisitos de incorporación.

ÁREA ANALIZADA

Las condiciones generales de contratación son un elemento dinámico, sometido a cambios durante su periodo de vigencia. Ello genera problemas en la prueba del contenido de sus cláusulas que un determinado usuario aceptó en una fecha concreta.

Al final de las CGC aparece un botón de validación mediante el cual el cliente declara haber leído y aceptado las CGC, pero siempre existe la incertidumbre sobre los medios de prueba que podrán utilizar ambas partes, en caso de controversia, para demostrar el contenido de las cláusulas que aceptaron.

Existen diversos sistemas para dicha actividad probatoria, entre los que destacan el Registro de condiciones generales de contratación, y los sistemas de auditoría externa, como CGC Audit y AENOR.

ACTIVIDAD PREVENTIVA

- Compruebe que en el formulario de pedido existe un enlace con las condiciones generales de contratación.
- Compruebe si en las condiciones generales de contratación o en el formulario de pedido existe un enlace con una sistemas de auditoría externa de CGC, como CGC Audit (<http://www.onnet.es/cgcaudit.htm>) o AENOR (<http://www.aenor.es>).

ACCIONES A REALIZAR

- Conserve un ejemplar en soporte duradero de las condiciones generales de contratación que rigen la adquisición del producto o la contratación del servicio.

LEGISLACIÓN APLICABLE

- .- Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13-4-1998, de condiciones generales de la contratación.
- .- Artículo 3. Confirmación documental de la contratación efectuada.
- .- Artículo 5. Atribución de la carga de la prueba.

ÁREA ANALIZADA

La contratación a través de Internet tiene a veces la paradoja de la rapidez del medio utilizado para la transacción y la lentitud del medio utilizado para la entrega. Ello se justifica, en el caso de productos físicos, por la necesidad de emplear sistemas logísticos económicos, que se aprovechen de rutas establecidas para la entrega de varios productos en un mismo envío. En cualquier caso, el usuario puede escoger entre sistemas de entrega rápidos, con un mayor coste, y sistemas de entrega normal, con un coste reducido.

Respecto al plazo de entrega, la Ley de Comercio Minorista es categórica, al establecer un plazo de treinta días para la entrega de los productos adquiridos a través de un sistema de venta a distancia, en el caso de que las partes no hayan pactado uno distinto.

ACTIVIDAD PREVENTIVA

- Compruebe los distintos sistemas de entrega disponibles, así como el coste y los plazos de entrega de cada uno.
- Compruebe si en las condiciones generales de contratación o en el formulario de pedido existe se menciona el plazo de entrega, y las consecuencias de un retraso en la entrega.

ACCIONES A REALIZAR

- Conserve un ejemplar en soporte duradero del formulario del comprobante de la transacción, en el que se mencione el plazo de entrega del producto adquirido.

LEGISLACIÓN APLICABLE

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.

.- Artículo 43: *Plazo de ejecución y pago.*

.- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.

.- Artículo 7: Ejecución.

ÁREA ANALIZADA

En el caso de productos que pueden suministrarse en formato digital, es posible efectuar la transferencia del bien a través de la propia red. Este es el caso de los programas de ordenador, las imágenes digitalizadas y las demás obras en forma binaria.

En el caso de los servicios, también es posible una forma de prestación a través de la red. Por ejemplo, en el caso de los servicios de bases de datos, traducción, auditoría, y cualquier otro trabajo que pueda efectuarse sin necesidad de un desplazamiento o un contacto personal.

En el caso de los productos físicos, es decir, todos aquellos bienes que no pueden ser entregados a través de la red, la forma de entrega será la pactada en la casilla correspondiente del formulario de pedido, pudiendo ésta ser cualquiera de las modalidades habituales en el comercio convencional, por ejemplo:

- Correo.
- Mensajería.
- Transporte por carretera.
- Avión.
- Etc.

En estos casos será importante establecer en el contrato la parte que se hará cargo de los costes de envío.

Un servicio adicional puede consistir en la posibilidad de consultar una base de datos on line, en la que el usuario pueda comprobar la situación de su pedido.

ACTIVIDAD PREVENTIVA

- Compruebe los distintos sistemas de entrega disponibles, así como el coste y los plazos de entrega de cada uno.
- Compruebe si en las condiciones generales de contratación o en el formulario de pedido existen o se mencionan las modalidades de entrega.

ACCIONES A REALIZAR

- Conserve un ejemplar en soporte duradero del formulario del comprobante de la transacción, en el que se mencione la forma de entrega del producto adquirido.

LEGISLACIÓN APLICABLE

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.

.- Artículo 43 - *Plazo de ejecución y pago.*

.- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia:

.- Artículo 7 - *Ejecución.*

3.5.6

Plazo de desistimiento

ÁREA ANALIZADA

La imposibilidad de apreciar directamente las cualidades de un producto físico comprado a través de Internet justifica la devolución del mismo si, en el momento de recibirlo, el comprador comprueba que no se ajusta a lo que él deseaba.

La Ley establece un plazo de siete días desde el momento de la recepción del producto para desistir del mismo y devolverlo al comercio que lo vendió.

ACTIVIDAD PREVENTIVA

- Solicite toda la información disponible del producto, consulte a otros usuarios del mismo y establezca todas las cautelas necesarias para impedir tener que ejercitar el derecho de desistimiento.
- Compruebe si en las condiciones generales de contratación o en el formulario de pedido se menciona el procedimiento para ejercitar el derecho de desistimiento.
- En el caso de adquirir productos en otros países, compruebe su suministrador ha contemplado la posibilidad de desistir de la compra en un plazo determinado.

ACCIONES A REALIZAR

- En el caso de comprobar, dentro de los siete días siguientes a la recepción del producto, que éste no se ajusta a las características prometidas o a las esperadas, puede tomar la decisión de devolverlo al suministrador.
- Si decide hacerlo, compruebe el procedimiento a seguir para remitirlo a su suministrador y conseguir el reembolso de la cantidad pagada.
- Si no existe procedimiento, proceda a enviarlo al domicilio de la persona física o jurídica que lo suministró mediante un sistema de entrega que le permita obtener un acuse de recibo o una prueba de la devolución del producto.

LEGISLACIÓN APLICABLE

- .- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.
- .- Artículo 44: *Derecho de desistimiento.*
- .- Artículo 45: *Excepciones al derecho de desistimiento.*

ÁREA ANALIZADA

Además del derecho de desistimiento, algunas empresas establecen la posibilidad de devolver el producto adquirido si se cumplen ciertas condiciones, por ejemplo, defectos aparecidos dentro del periodo de garantía.

Si la devolución se produce como resultado de ejercitar el derecho de desistimiento, existen algunos productos que están excluidos del derecho a devolución.

ACTIVIDAD PREVENTIVA

- Compruebe si en las condiciones generales de contratación o en el formulario de pedido se menciona el procedimiento y los requisitos que se deben cumplir para efectuar devoluciones.
- Compruebe los supuestos que se hallan excluidos del derecho a devolución.
- Compruebe el régimen de la garantía.
- Compruebe quién debe asumir los gastos derivados de la devolución.
- Si la devolución se produce como resultado de ejercitar el derecho de desistimiento, compruebe si el producto adquirido está excluido por ley del derecho a devolución.

LEGISLACIÓN APLICABLE

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.

.- Artículo 44: *Derecho de desistimiento*.

.- Artículo 45: *Excepciones al derecho de desistimiento*.

ÁREA ANALIZADA

Al igual que los productos adquiridos en comercios presenciales, los bienes que se compran a través de Internet disponen de un plazo de garantía durante el cual el fabricante se obliga a la subsanación de defectos o la sustitución del producto.

ACTIVIDAD PREVENTIVA

- Compruebe si en las condiciones generales de contratación o en el formulario de pedido se menciona el plazo de garantía.
- Compruebe los derechos que le concede la garantía
- Compruebe el procedimiento y los requisitos que se deben cumplir para ejercitar la garantía.
- Compruebe los supuestos que se hallan excluidos de la garantía.

LEGISLACIÓN APLICABLE

- .- Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios:
- .- Artículo 11.

ÁREA ANALIZADA

Los contratos referidos a productos financieros consistentes en servicios de inversión, instituciones de inversión colectiva, seguro y reaseguro, bancarios o prestados por entidades sujetas a supervisión, relativos a fondos de pensiones y a operaciones a plazo y de opción no se hallan sujetos a las obligaciones establecidas para la contratación electrónica con condiciones generales de contratación.

No obstante, en este tipo de servicios, deberá quedar constancia documental de la contratación efectuada, ya sea en forma escrita o en registros magnéticos o informáticos, de acuerdo con la normativa específica aplicable en cada caso. A falta de ésta, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.

ACTIVIDAD PREVENTIVA

- Antes de establecer contacto con una entidad que ofrece productos a través de Internet, compruebe desde qué país está operando.
- En caso de tratarse de una entidad extranjera, consulte la ficha correspondiente a productos financieros extranjeros ofrecidos a través de Internet.

ACCIONES A REALIZAR

- Identificación clara de la entidad financiera.
- Revisión de las condiciones generales de contratación.
- Solicitud de constancia documental de la contratación efectuada.

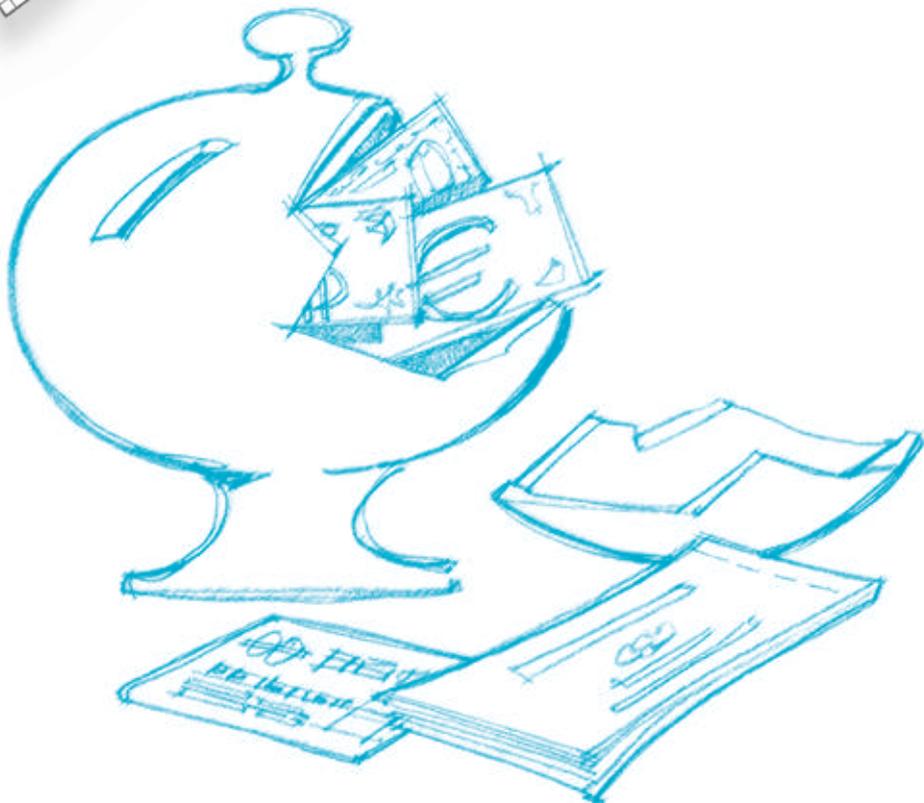
LEGISLACIÓN APLICABLE

- .- Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13-4-1998, de condiciones generales de la contratación:
- .- Artículo 1.3.

3/6

área

Medios de pago



3.6.1

Cargo indebido en tarjeta de crédito

ÁREA ANALIZADA

Existe la creencia generalizada de que es arriesgado facilitar los datos de una tarjeta de crédito a través de Internet, ya que existe la posibilidad de que la transmisión sea interceptada y el número de la tarjeta capturado por personas que pretendan utilizarlo con fines fraudulentos. Aunque la posibilidad de que ello ocurra es muy reducida, la normativa que regula la venta a distancia en el ámbito europeo ha dispuesto una serie de cautelas para defender al consumidor de este tipo de riesgos, ofreciéndole la posibilidad de anular los cargos efectuados sin su consentimiento expreso.

ACTIVIDAD PREVENTIVA

- Evite los comercios virtuales en los que el oferente no está identificado.
- Compruebe que el entorno donde realiza la transacción es seguro.
- Para ello, busque el símbolo correspondiente en su navegador (candado cerrado).
- Compruebe que el comercio oferente dispone de un certificado que lo identifica.
- Compruebe el país en el que está ubicado el comercio.
- Tenga en cuenta los problemas de reclamación en paraísos fiscales.
- Guarde los comprobantes de todas sus compras con tarjeta.
- Imprima las páginas de confirmación de sus pedidos a través de Internet.
- Compruebe periódicamente los extractos de sus tarjetas.
- Comunique inmediatamente a su entidad financiera cualquier irregularidad.

ACCIONES A REALIZAR EN CASO DE CARGO INDEBIDO

- Comunique inmediatamente a su entidad financiera la existencia del cargo indebido.
- Utilice el teléfono para una comunicación rápida solicitando la anulación del cargo.
- Envíe un telegrama a la entidad financiera para dejar constancia de la orden.
- Compruebe la efectividad de la anulación durante los tres días siguientes.

LEGISLACIÓN APLICABLE

.- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.

.- Artículo 46: *Pago mediante tarjeta de crédito.*

.- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.

- Artículo 8: *Pago mediante tarjeta.*

ÁREA ANALIZADA

La mayoría de las páginas web dedicadas al comercio electrónico utilizan el protocolo de seguridad SSL, que permite establecer un canal cifrado entre el servidor del comercio y el navegador del cliente. Los servidores que utilizan este protocolo de seguridad son los llamados servidores seguros, y se distinguen porque en el navegador aparece un candado cerrado, que indica que se ha abierto una sesión SSL que garantiza la confidencialidad de la transacción.

ACTIVIDAD PREVENTIVA

- Compruebe que el formulario de pedido en el que se solicitan los datos de su tarjeta de crédito, está utilizando un servidor seguro, y que el icono del candado cerrado aparece en su navegador.
- En la medida de lo posible, intente realizar sus pedidos a través de comercios que utilicen servidores seguros.

ACCIONES A REALIZAR

- Si el formulario en los que se recaban los datos de su tarjeta de crédito no utiliza un servidor seguro y, por lo tanto, no se visualiza el icono del candado cerrado en su navegador, sea consciente de que la confidencialidad de los datos no está garantizada.

LEGISLACIÓN APLICABLE

- .- Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista.
- .- Artículo 46: *Pago mediante tarjeta de crédito.*

ÁREA ANALIZADA

El Real Decreto Ley 14/1999 establece la equiparación de la firma electrónica avanzada a la firma manuscrita, con idénticos efectos jurídicos y validez probatoria.

Uno de los principales inconvenientes de la implantación de la firma electrónica avanzada es la inexistencia de un mercado de usuarios certificados al que una empresa dedicada al comercio electrónico pueda dirigir su oferta. Ello obligará a que, durante un tiempo, coexistan los modelos transaccionales no certificados con los descritos en el nuevo marco jurídico de la firma electrónica.

ACTIVIDAD PREVENTIVA

- Solicite el uso de firma electrónica avanzada en aquellas transacciones electrónicas en las que la cuantía sea elevada (Por ejemplo, más de 500.000 pesetas) o desee garantizar los principios de autenticidad, integridad y no repudio.
- En el caso de disponer de los elementos necesarios para utilizar la firma electrónica, aplique las medidas de seguridad necesarias para evitar un uso no autorizado por parte de terceros.
- Siga los consejos de seguridad suministrados por la entidad financiera y la entidad de certificación que han participado en el proceso de identificación y emisión del certificado.

ACCIONES A REALIZAR

- En el caso de no disponer de los elementos necesarios para utilizar la firma electrónica, compruebe el tipo de certificados y los sistemas de pago con firma electrónica que aceptan sus proveedores habituales y diríjase a su entidad financiera o directamente a la entidad de certificación correspondiente para solicitarlos.

LEGISLACIÓN APLICABLE

- .- Real Decreto-Ley 14/1999, de 17 de septiembre de 1999. Firma Electrónica.
- .- Artículo 3. Efectos jurídicos de la firma electrónica.
- .- Sentencia del Tribunal Supremo de 3 de noviembre de 1997.

ÁREA ANALIZADA

Es evidente que la transacción debe ser el centro de atención de cualquier protocolo de seguridad, pero los usuarios no deben olvidar que también tendrán que establecer las correspondientes cautelas en la conservación de los elementos que intervienen en la operación, o que son el resultado de la misma. Nos referimos al PIN, a los certificados, las claves privadas y los demás elementos de seguridad cuya custodia corresponde al usuario y, en otro nivel, a los documentos electrónicos almacenados en el ordenador tras las fases de validación y confirmación de la transacción.

Si el certificado electrónico ha sido en el navegador del PC del usuario, éste debe mantener unas medidas de seguridad esenciales que impidan el acceso a los dispositivos que permitirían suplantar su identidad.

ACTIVIDAD PREVENTIVA

- En el caso de que el certificado se halle en una tarjeta inteligente, ésta deberá permanecer siempre en poder del usuario, evitando dejarla insertada en la ranura del lector de tarjetas.
- Deben evitarse los sistemas de memorización automática de la contraseña o PIN.
- En la oficina, configure el protector de pantalla de su ordenador con una contraseña para impedir el acceso al mismo cuando se ausente de su puesto de trabajo.
- Extreme sus precauciones con los ordenadores portátiles cuando esté de viaje.
- Cuando no se opere con el ordenador propio, debe evitarse la utilización de sistemas que no merezcan confianza, en los que pueda existir algún mecanismo de explotación. de la memoria caché o cualquier otro dispositivo que permita extraer, copiar o memorizar alguno de los elementos de seguridad utilizados por el usuario.

ACCIONES A REALIZAR

- Comunique cualquier incidente de seguridad o circunstancia sospechosa a la entidad que le entregó el certificado electrónico o el identificador y la contraseña.

LEGISLACIÓN APLICABLE

- .- Real Decreto-Ley 14/1999, de 17 de septiembre de 1999. Firma Electrónica.
- .- Artículo 3. Efectos jurídicos de la firma electrónica.
- .- Sentencia del Tribunal Supremo de 3 de noviembre de 1997.

3/7

área

Fiscalidad



ÁREA ANALIZADA

Cuando se efectúa una transacción a través de Internet se produce una transferencia de dinero a favor del vendedor del producto o prestador del servicio que, en algunas ocasiones, genera la obligación para el comprador o usuario, de retener un porcentaje a cuenta del impuesto que la otra parte deberá pagar por los beneficios obtenidos durante el ejercicio.

Esta obligación puede surgir, entre otros, en los siguientes supuestos:

- Pago de servicios a un profesional español.
- Pago de servicios a un profesional o empresa extranjera.
- Pago de un canon de propiedad intelectual.
- Etc.

ACTIVIDAD PREVENTIVA

- Compruebe si el pago que va a realizar está sujeto a retención.
- Solicite asesoramiento a la entidad financiera que va a realizar la transferencia.

ACCIONES A REALIZAR

- En el caso de que el pago a realizar esté sujeto a retención y el beneficiario del mismo no lo haya indicado así en su factura, solicite que rectifique la factura.
- Una vez realizada la retención, la cantidad retenida debe ser liquidada en su Delegación de Hacienda. Solicite información sobre el impreso que debe utilizar para ello, ya que es diferente en función del carácter nacional o extranjero del sujeto pasivo al que se ha practicado la retención.

LEGISLACIÓN APLICABLE

- .- Legislación sobre el Impuesto de la Renta de las Personas Físicas.
- .- Legislación sobre el Impuesto de Sociedades.
- .- Legislación sobre tributación de no residentes.
- .- Convenios de doble imposición con otros países.

ÁREA ANALIZADA

La actividad comercial desarrollada a través de Internet está sujeta a impuestos indirectos, al igual que en el mercado presencial.

La principal diferencia es que, además de contratar productos físicos que se entregan por los medios tradicionales, pueden adquirirse productos en formato digital, que se descargan a través de la propia red. Es en este caso cuando se produce un trato discriminatorio en materia de IVA, y se considera que dicha prestación no es un producto, sino un servicio. La consecuencia directa de este régimen para el usuario es una mayor carga impositiva. Por ejemplo, si un usuario compra un libro a través de Internet, pagará el IVA correspondiente al tipo reducido de los libros (4%), pero si esa misma obra la adquiere en formato digital a través de Internet, pagará el IVA correspondiente a servicios (16%).

Por otra parte, existen obligaciones adicionales de liquidación del IVA en la contratación de ciertos servicios de telecomunicación en países no miembros de la Unión Europea.

ACTIVIDAD PREVENTIVA

- En el caso de contratar un servicio de telecomunicaciones en un país que no pertenezca a la Unión Europea, compruebe si tiene la obligación de liquidar igualmente el IVA en España.
- Solicite asesoramiento a su asesor fiscal o Delegación de Hacienda.

ACCIONES A REALIZAR

- Una vez realizada la contratación de un servicio de telecomunicaciones previsto en el Real Decreto Ley 14/1997, la cantidad correspondiente al IVA español debe ser liquidada en su Delegación de Hacienda. Solicite información sobre el impreso que debe utilizar para ello.

LEGISLACIÓN APLICABLE

- .- Legislación sobre el Impuesto del Valor Añadido.
- .- Real Decreto Ley 14/1997.
- .- Decisión del Consejo de 17 de marzo de 1997.

ÁREA ANALIZADA

El Real Decreto Ley 14/1999 establece la equiparación de la firma electrónica avanzada a la compra de productos adquiridos en el extranjero a través de Internet puede suponer una importación sujeta al pago de un arancel.

En el caso de productos físicos, el hecho de que la contratación se haya realizado a través de la red no modifica esta obligación. La importación de productos se produce de la misma manera que en una contratación tradicional.

En el caso de los productos en formato digital, que se descargan a través de la propia red, el caso es distinto, ya que la modalidad de transmisión escapa al control estatal. Este tráfico transfronterizo está sujeto en algunos países a una moratoria, durante la cual no existe la obligación de liquidar aranceles.

ACTIVIDAD PREVENTIVA

- En el caso de adquirir productos en un país que no pertenezca a la Unión Europea, compruebe si tiene la obligación de pagar algún arancel.
- Solicite asesoramiento a su asesor fiscal o transitario.

ACCIONES A REALIZAR

- En el caso de confirmar que la importación del producto está sujeta a arancel, solicite asesoramiento sobre la forma de proceder a los tramites de importación y a la liquidación del arancel correspondiente.

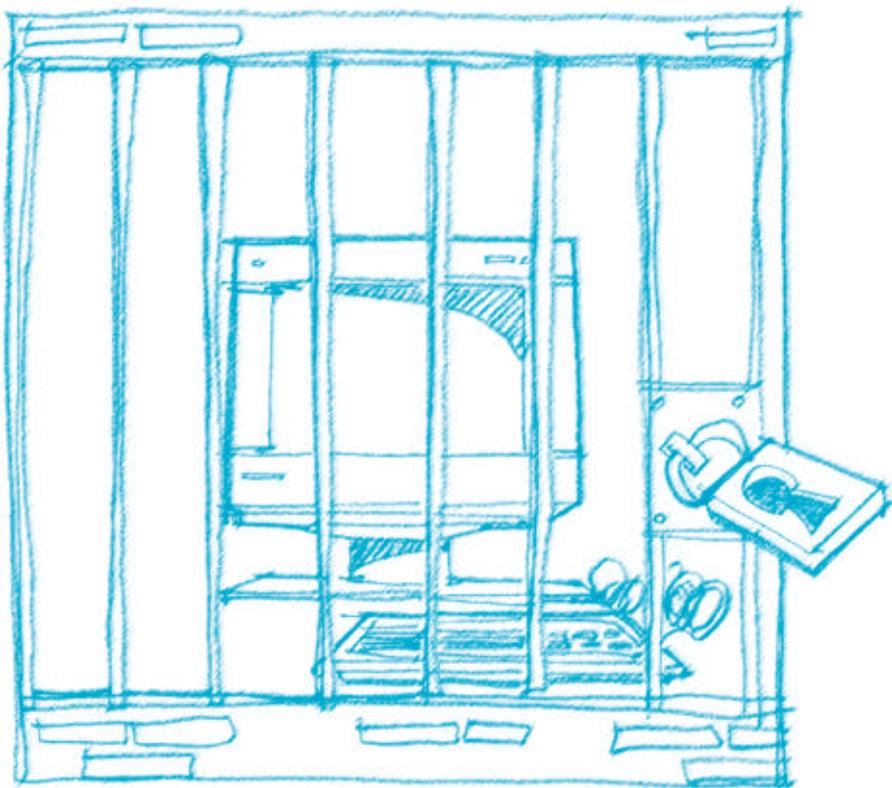
LEGISLACIÓN APLICABLE

.- Legislación sobre aranceles aduaneros.

3/8

área

Responsabilidad Civil



3.8.1

Productos defectuosos

ÁREA ANALIZADA

Los productos adquiridos a través de Internet están sujetos a las mismas incidencias que los adquiridos a través de sistemas tradicionales. Por lo tanto, el régimen aplicable en el caso de comprar un producto defectuoso es exactamente el mismo, incluyendo las medidas preventivas a adoptar y las reclamaciones que pueden realizarse.

El valor añadido que aporta Internet es la posibilidad de obtener mayor información de un producto antes de adquirirlo, y contrastar experiencias con otros consumidores del mismo producto para conocer su grado de satisfacción.

Existe también la posibilidad de que, una vez detectado un defecto, el propio fabricante se ponga en contacto más fácilmente con los consumidores afectados y les informe sobre el procedimiento de subsanación. En otros casos, son los propios usuarios los que colaboran entre sí para transmitir instrucciones sobre la forma de proceder ante un determinado producto o fabricante.

ACTIVIDAD PREVENTIVA

- Antes de adquirir un producto de una cuantía considerable, compruebe previamente si existe un club de usuarios donde pueda contrastar aspectos relativos a la calidad del mismo y a la posible existencia de defectos.

ACCIONES A REALIZAR

- En el caso de detectar un defecto en un producto adquirido a través de Internet:
 - Póngase en contacto inmediatamente con su suministrador para ver si se trata de un defecto ya conocido y existe un procedimiento específico para su subsanación.
 - Pida asesoramiento a una asociación de usuarios si no recibe el trato apropiado por parte del suministrador.
 - Compruebe si existe algún foro de consumidores en el que pueda contrastar su experiencia con otros usuarios del mismo producto.

LEGISLACIÓN APLICABLE

.- Código Civil: Artículos 1902, 1101,1102,1103, 1104, 1105 y 1106.

ÁREA ANALIZADA

Constantemente se publican en los medios de comunicación noticias sobre la aparición de nuevos virus capaces de destruir información en un sistema informático. Internet ha permitido una mayor transmisión de virus, a causa de la mayor facilidad para transmitir programas y ficheros.

Existen muchos tipos de virus, aunque los que habitualmente se transmiten a través de la red, pueden agruparse en tres grandes grupos:

- Virus que van en otros programas comerciales, generalmente copias no autorizadas.
- Ficheros ejecutables que se envían por correo electrónico y que, en algunos casos se propagan utilizando la lista de direcciones de correo electrónico del propio usuario. (Melissa, Pretty Park, I Love you).
- Macros residentes en documentos como hojas de cálculo, textos, etc.

La transmisión de un virus es el resultado de una cadena de responsabilidades que llega hasta el propio usuario, por no haber instalado o actualizado un programa capaz de detectar y neutralizar virus informáticos. En algunos casos, el virus es tan reciente, que no existen librerías de programas anti-virus que lo hayan previsto, por lo que se trata más de un caso de fuerza mayor inevitable, que de negligencia.

ACTIVIDAD PREVENTIVA

- Adquiera siempre programas originales.
- No acepte ni transmita copias no autorizadas de programas de ordenador.
- No instale programas obtenidos en fuentes no fiables.
- No ejecute ningún fichero sospechoso que reciba por correo electrónico, aunque provenga de un amigo.
- Instale y mantenga actualizado un programa anti-virus.
- Suscriba un servicio de alerta de virus en Internet.

ACCIONES A REALIZAR

- En el caso de conocer la existencia de un nuevo virus solicite inmediatamente una actualización del programa antivirus a su proveedor habitual.

LEGISLACIÓN APLICABLE

.- Código Civil: Artículos 1902, 1101,1102,1103, 1104, 1105 y 1106.

ÁREA ANALIZADA

En un entorno tan cambiante como Internet, resulta conveniente plantearse las posibles consecuencias de una decisión basada en datos obsoletos obtenidos en una página web. Para analizarlo, debemos distinguir entre la información sometida a constantes cambios y la información estática.

Los programas navegadores más utilizados, como Microsoft Explorer y Netscape, crean un directorio en el disco duro del ordenador en el que van almacenando de forma automática los archivos de imágenes, texto, botones de navegación, texturas de fondo, etc. que van visualizando en una página web. De esta manera, si los contenidos de ese directorio no son borrados por el usuario, el navegador los utiliza como memoria caché, es decir, cuando debe presentar en pantalla algún archivo que ya ha sido visualizado previamente, acude a la caché para evitar tener que transferirlo de nuevo desde el servidor remoto hasta el ordenador del usuario. Esta función también la realizan los servidores y encaminadores situados como nodos intermedios entre el servidor del usuario y el servidor donde se encuentra la página web visitada. Con ello se gana rapidez en la navegación por Internet, ya que los contenidos visualizados previamente por unos usuarios pueden ser descargados desde servidores más cercanos por otros usuarios que se hallen en la misma zona.

No obstante, el idéntico formato o denominación del archivo guardado en la caché y el del servidor, genera riesgos en el caso de información cuya frecuencia de actualización es muy alta, ya que el navegador puede presentar en pantalla una información no actualizada. Ello puede hacer que el usuario asuma dichos datos como actuales y tome una decisión basada en una información errónea.

Si se trata de un servicio cuyos precios se actualizan cada cuarto de hora, o incluso cada minuto, y el usuario está en línea durante un tiempo superior y no actualiza la pantalla, el riesgo de error también aparece, aunque en este caso no haya intervenido la caché.

En cualquier caso, los proveedores que suministran información que está sometida a cambios constantes, acostumar a configurar su página web para que la actualización se produzca sin el concurso del usuario. Las entidades que realizan esta actividad acostumbra a enervar su responsabilidad introduciendo en sus páginas web una advertencia al usuario para que pulse el botón de "reload", "refresh" o actualización de la pantalla antes de tomar una decisión basada en los datos suministrados.

Se hallan en esta situación todos aquellos servicios que facilitan precios o tarifas en tiempo real, información bursátil, resultados electorales, noticias en línea, venta de localidades, reservas de viajes, reservas hoteleras y cualquier otra información que esté sometida a un alto nivel de modificación.

Por su parte, el usuario tiene la responsabilidad de actualizar la información antes de realizar una compra o tomar una decisión basada en un dato que puede haber cambiado desde el momento en que lo consultó por última vez.

En el caso de informes, estadísticas, leyes y cualquier información localizada en una página web con una mayor vocación de perdurabilidad, pero con igual nivel de riesgo si no se encuentra actualizada, es habitual mencionar en qué fecha ha sido introducida en la red o cuando se actualizó por última vez, de manera que pueda deducirse su vigencia.

Información no actualizada

Existen páginas que no han sido actualizadas en años, y a la velocidad que va Internet, puede decirse que visitarlas es pura arqueología. Son zonas abandonadas que vamos encontrando al navegar por la red. El usuario debe tener la cautela de comprobar el nivel de actualización de un dato obtenido a través de Internet antes de tomar una decisión basada en algo que ya es historia.

ACTIVIDAD PREVENTIVA

- Compruebe el nivel de actualización de cualquier información que obtenga a través de Internet.
- Si consulta una norma jurídica a través de Internet, compruebe que no esté derogada.
- Cuando consulte periódicamente el contenido de una página web cuyos datos se modifican constantemente, pulse el botón de su navegador que tenga asignada la función de actualizar los contenidos visualizados en la pantalla.
- Configure su navegador para que actualice de forma automática los contenidos de la memoria caché.
- Si ha cargado una página web para poder visualizarla posteriormente sin conexión a la red (navegación "off line"), recuerde actualizar los contenidos antes de tomar una decisión basada en dicha información.

ACCIONES A REALIZAR

- Antes de adquirir un producto o tomar una decisión basada en datos que pueden haber perdido vigencia, realice una actualización de los mismos.

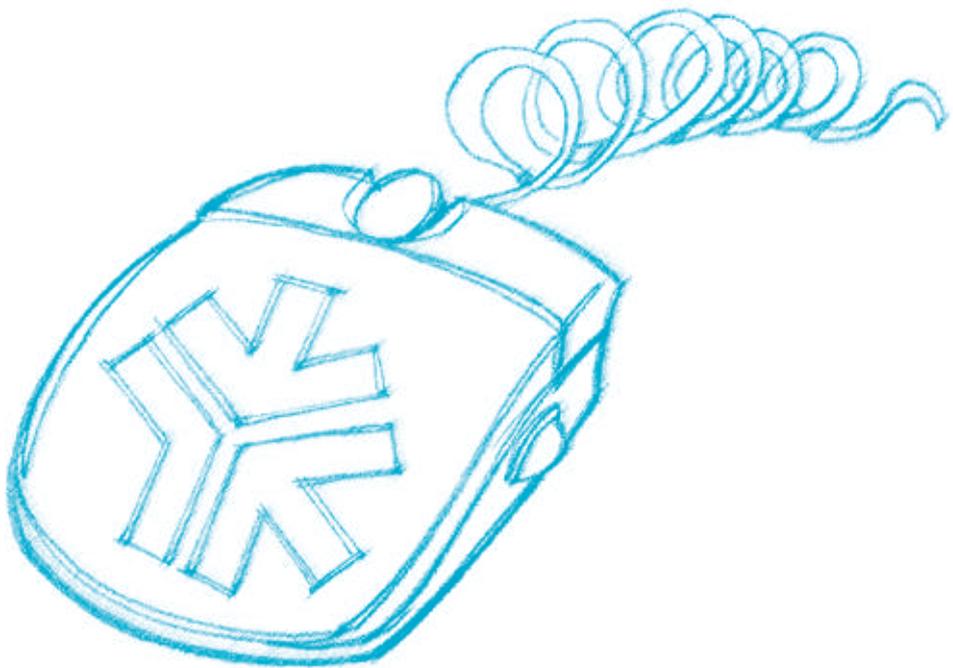
LEGISLACIÓN APLICABLE

.- Código Civil: Artículos 1902, 1101,1102,1103, 1104, 1105 y 1106.

3/9

área

Resolución de Controversias



ÁREA ANALIZADA

El sistema arbitral de consumo es una vía extrajudicial, rápida, eficaz y económica que permite resolver con carácter vinculante y ejecutivo los desacuerdos de los consumidores y usuarios con los vendedores o prestadores de servicios:

- Es un sistema rápido, ya que la resolución debe dictarse en el plazo máximo de 4 meses desde la designación del Colegio Arbitral.
- Es un sistema eficaz, que resuelve las cuestiones mediante una resolución arbitral, denominada laudo, sin necesidad de recurrir a la vía judicial.
- Es un sistema económico, gratuito para las partes, salvo en algunos casos la práctica de peritajes.
- Es un sistema voluntario, ya que ambas partes se adhieren libremente al mismo para quedar vinculadas a las resoluciones.
- Es un sistema ejecutivo, porque los laudos son de aplicación obligatoria.

ACTIVIDAD PREVENTIVA

- Compruebe si el comercio al que va adquirir un producto está adherido al arbitraje de consumo. Si el empresario o el profesional se adhiere al sistema arbitral de consumo, podrá exhibir un distintivo oficial, que indica la oferta de una garantía añadida a los servicios que presta habitualmente. Para los consumidores este símbolo nos supone una garantía de resolver rápidamente los desacuerdos que puedan producirse con la empresa adherida al sistema arbitral.

ACCIONES A REALIZAR EN CASO DE CONTROVERSIA

- Presente la correspondiente reclamación o solicitud de arbitraje ante la Junta arbitral de consumo de su municipio o comunidad autónoma.

LEGISLACIÓN APLICABLE

- .- Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios:
- .- Disposición Adicional Primera.
- .- Real Decreto 636/1993, de 3 de mayo, por el que se regula el Sistema Arbitral de Consumo.
- .- Ley 36/1988, de 5 de diciembre. Régimen Jurídico del Arbitraje.

ÁREA ANALIZADA

La Directiva de Comercio Electrónico defiende la figura del arbitraje especializado como medio ideal para la resolución de las controversias que las operaciones de comercio electrónico puedan originar. Ello resuelve también el problema de la determinación de la jurisdicción aplicable en el caso de operaciones transfronterizas.

La Comisión Europea está impulsando la creación de una red de organismos arbitrales en cada estado miembro de la Unión Europea, que estén preparados para resolver conflictos derivados del comercio electrónico de forma rápida y económica. El objetivo final es que este arbitraje pueda realizarse a través de la propia red, eliminando los problemas de desplazamientos y acelerando el procedimiento.

ACTIVIDAD PREVENTIVA

- Compruebe si en su lugar de residencia existen organismos que realicen arbitraje telemático especializado en comercio electrónico, de acuerdo con las pautas creadas por la Comisión Europea.
- Acuda preferentemente a los comercios que sometan las divergencias surgidas con sus clientes al sistema arbitral promovido por la Comisión Europea en materia.
- Recuerde que las cláusulas que sometan la controversia a una entidad arbitral no reconocida pueden ser declaradas nulas.

ACCIONES A REALIZAR EN CASO DE CONTROVERSIAS

- Compruebe si las condiciones generales de contratación incluyen una cláusula de arbitraje.
- En caso positivo, presente el correspondiente escrito introductorio en el tribunal u organismo arbitral mencionado en la cláusula o convenio arbitral.

LEGISLACIÓN APLICABLE

- .- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el Mercado Interior (Directiva sobre el Comercio Electrónico):
<http://www.aece.org/legislacion/DirectivaCE.pdf>
- .- Ley 36/1988, de 5 de diciembre. Régimen Jurídico del Arbitraje.
- .- Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios:
- .- Disposición Adicional Primera.

ÁREA ANALIZADA

Las condiciones generales de contratación que las partes aceptan en el momento de realizar una transacción de comercio electrónico contienen, en la mayoría de los casos, una cláusula en la que se establece cuál va a ser la legislación aplicable a dicha operación y cuál va a ser la jurisdicción competente en caso de litigio.

Aunque la escasa cuantía de las transacciones realizadas a través de Internet hacen que el consumidor no valore la trascendencia de este tipo de cláusulas, es importante tenerlas en cuenta en aquellos productos que pueden causar daños en caso de ser defectuosos.

ACTIVIDAD PREVENTIVA

- Antes de efectuar la transacción, compruebe si las condiciones generales de contratación incluyen una cláusula de sumisión expresa.

ACCIONES A REALIZAR EN CASO DE CONTROVERSIA

- Compruebe si las condiciones generales de contratación incluyen una cláusula de sumisión expresa.
- En caso positivo, compruebe a qué tribunales se han sometido las partes y analice la conveniencia de presentar la reclamación en dicha sede.
- Recuerde que los pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor pueden ser declarados nulos.

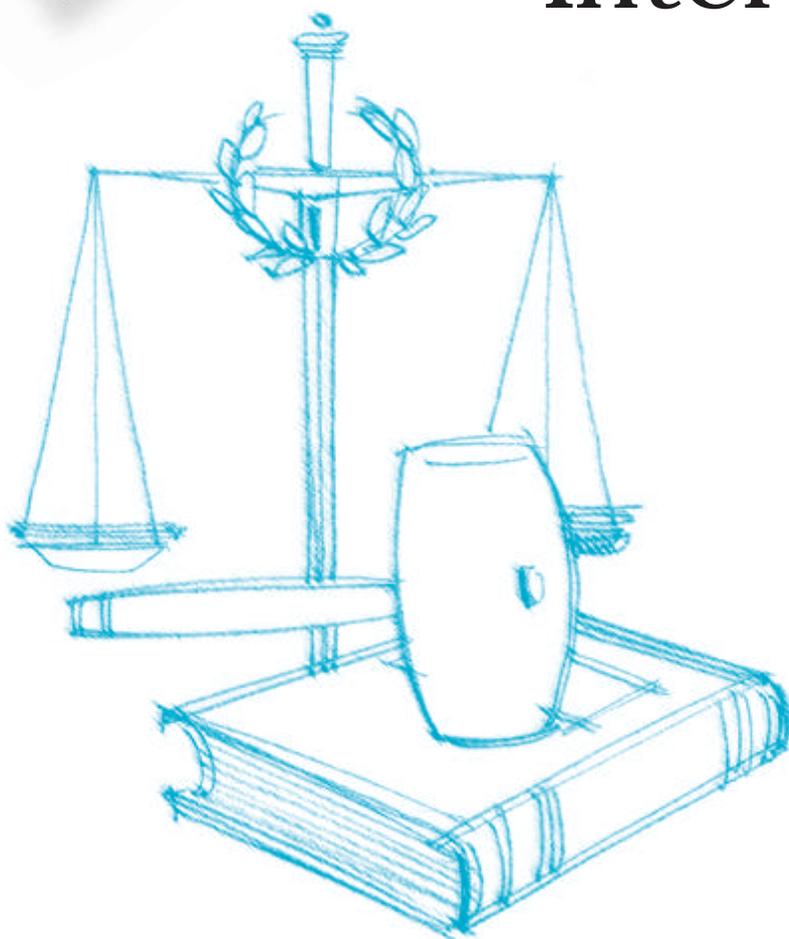
LEGISLACIÓN APLICABLE

- .- Ley 36/1988, de 5 de diciembre. Régimen Jurídico del Arbitraje.
- .- Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios:
- .- Disposición Adicional Primera.

3/10

área

Fraudes y Delitos en Internet



ÁREA ANALIZADA

El riesgo de ser víctima de un delito de estafa en Internet es similar al que existe en las relaciones presenciales. La principal diferencia consiste en la virtualidad. Ésta tiene dos importantes consecuencias:

1. Al no existir contacto presencial no se pueden analizar una serie de factores que en condiciones normales alertarían a la víctima sobre el posible engaño (Respecto al producto: existencia, calidad, disponibilidad).
(Respecto al oferente: confianza, apariencia, establecimiento permanente).
2. Posibilidad de que la estafa se consume sin la participación simultánea de ambas partes en la transacción.
(Ausencia del oferente: el comprador adquiere un producto inexistente en una página web).
(Ausencia del comprador: el oferente simula una transacción con los datos del comprador).

La actividad descrita en el artículo 248.2 del Código Penal no exige que la concurrencia de engaño, es decir, es posible calificar como estafa cualquier manipulación informática que se realice con ánimo de lucro y genere una disposición patrimonial in consentida.

ACTIVIDAD PREVENTIVA

- Establezca las medidas de seguridad oportunas para evitar sustracciones de contraseñas y suplantaciones de identidad en transacciones electrónicas.
- No conteste a ningún mensaje o comunicación en la que se soliciten sus datos identificativos y contraseñas.
- No siga las instrucciones de ninguna persona desconocida que impliquen cambios de configuración en los elementos de seguridad de su sistema informático, navegador, etc.
- Extreme las precauciones en los casos en que se solicite una contrapartida económica importante para la contratación de cualquier producto o servicio a través de Internet.
- En la medida de lo posible, compruebe el certificado electrónico de la otra parte o solicite información adicional sobre su identidad.
- No participe en ninguna transacción en la que las partes no estén identificadas y le ofrezcan confianza.
- Instruya a los miembros de su familia para que adopten las mismas precauciones.

ACCIONES A REALIZAR

1. En el caso de detectar indicios de una posible estafa, ponga el hecho en conocimiento de un abogado especializado en delitos en Internet.
2. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 248.

ÁREA ANALIZADA

Aunque las posibilidades son mínimas, es importante que el usuario de Internet esté preparado para rechazar cualquier ataque contra la seguridad de su ordenador. No se trata sólo de la posibilidad de que otro usuario entre de forma no autorizada en su ordenador, sino del riesgo real de introducción de un virus informático que destruya información que puede resultar valiosa.

ACTIVIDAD PREVENTIVA

- Mantenga actualizado su programa antivirus, con el fin de incorporar los virus que se distribuyen a través de Internet.
- No abra archivos ejecutables que provengan de fuentes desconocidas o poco fiables.
- Si es un usuario habitual de los debates en tiempo real (chat), utilice regularmente programas detectores de caballos de Troya y de cualquier otra utilidad que permita a un usuario externo asumir el control de su ordenador. (Netbus, Back Orifice, etc.).
- No acepte programas que no sean originales y de fuentes fiables.

ACCIONES A REALIZAR

1. En el caso de detectar indicios de una posible estafa, ponga el hecho en conocimiento de un abogado especializado en delitos en Internet.
2. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 264.

ÁREA ANALIZADA

En condiciones normales, es poco probable el uso no autorizado de un sistema informático doméstico con conexión a Internet, ya que ello implicaría un acceso físico a la habitación donde se encuentre el ordenador, y esta posibilidad está restringida a un círculo limitado de personas, que merecen la confianza del usuario, o que están sujetas a una supervisión.

El riesgo se produce durante la conexión a Internet, si se produce un acceso no autorizado que persiga la finalidad de utilizar el ordenador atacado como plataforma para otras actividades. Aunque ello es improbable en las conexiones domésticas, debido a la temporalidad de la conexión y a la asignación de una dirección IP dinámica, que cambia en cada conexión, es menos extraña en una conexión permanente, mediante cable o red local.

ACTIVIDAD PREVENTIVA

- Si dispone de una conexión permanente a Internet, solicite información sobre las medidas de seguridad que puede establecer para impedir accesos no autorizados.
- No abra archivos ejecutables que provengan de fuentes desconocidas o poco fiables.
- Si es un usuario habitual de los debates en tiempo real (chat), utilice regularmente programas detectores de caballos de Troya y de cualquier otra utilidad que permita a un usuario externo asumir el control de su ordenador. (Netbus, Back Orifice, etc.)
- En la oficina, configure el protector de pantalla de su ordenador con una contraseña para impedir el acceso al mismo cuando se ausente de su puesto de trabajo.
- Tenga especial cuidado con los ordenadores portátiles cuando se halle de viaje.

ACCIONES A REALIZAR

1. En el caso de detectar indicios de una posible estafa, ponga el hecho en conocimiento de un abogado especializado en delitos en Internet.
2. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 256.

ÁREA ANALIZADA

Se trata de uno de los supuestos menos frecuentes, pero sobre el que hay que extremar las precauciones, debido al perjuicio sufrido incide directamente en una cantidad líquida de dinero.

Dada la seguridad actual de las plataformas de banca electrónica, resulta conveniente reforzar la seguridad del usuario, haciendo que los hábitos de conducta en Internet incluyan unas normas de seguridad que garanticen la ausencia de incidencias en este ámbito.

ACTIVIDAD PREVENTIVA

- Cumpla todas las obligaciones de seguridad establecidas en su contrato de banca electrónica.
- Establezca las medidas de seguridad oportunas para evitar sustracciones de contraseñas y suplantaciones de identidad en transacciones electrónicas.
- No conteste a ningún mensaje o comunicación en la que se soliciten sus datos identificativos y contraseñas.
- No siga las instrucciones de ninguna persona desconocida que impliquen cambios de configuración en los elementos de seguridad de su sistema informático, navegador, etc.
- Deben evitarse los sistemas de memorización automática de la contraseña o PIN.
- En la oficina, configure el protector de pantalla de su ordenador con una contraseña para impedir el acceso al mismo cuando se ausente de su puesto de trabajo.
- Extreme sus precauciones con los ordenadores portátiles cuando esté de viaje.
- Cuando no se opere con el ordenador propio, debe evitarse la utilización de sistemas que no merezcan confianza, en los que pueda existir algún mecanismo de explotación de la memoria caché o cualquier otro dispositivo que permita extraer, copiar o memorizar alguno de los elementos de seguridad utilizados por el usuario.

ACCIONES A REALIZAR

- En el caso de detectar indicios de una posible transferencia no autorizada de fondos de su cuenta, ponga el hecho en conocimiento de su banco o caja y, si lo considera necesario, acuda a un abogado especializado en delitos en Internet.

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 248.

ÁREA ANALIZADA

El diseño inicial del correo electrónico en Internet no incluyó la posibilidad de preservar la confidencialidad. La prioridad era conseguir que el mensaje llegase a su destinatario, y que lo hiciese lo más rápidamente posible.

El usuario debe ser consciente de que cada mensaje que envía o recibe va abierto, es decir, puede ser leído por cualquier persona que tenga conocimientos para ello y utilice programas que están al alcance de todo el mundo en la propia red. Dicha actividad constituye un delito equivalente a la apertura de correspondencia ajena.

No obstante, la gran cantidad de mensajes que se envían a lo largo del día a través de Internet hace poco probable que sea justamente el nuestro el interceptado.

Aun así, conviene aplicar ciertas cautelas en el momento de utilizar el correo electrónico a través de Internet.

ACTIVIDAD PREVENTIVA

- Sea consciente de que los mensajes que envía o recibe a través de Internet pueden ser leídos por otras personas.
- En la medida de lo posible, no utilice Internet para el envío de información que considere extremadamente confidencial.
- Si tiene que utilizar el correo electrónico para enviar información que considera confidencial, puede utilizar técnicas de cifrado para ocultar el contenido del mensaje.

ACCIONES A REALIZAR

1. Instale un programa de cifrado que añada la función de cifrar mensajes a su programa de correo electrónico.
2. Utilice un sistema de cifrado en los casos en que desee impedir el acceso al contenido de un mensaje de correo electrónico.
3. En el caso de detectar indicios de un posible delito de interceptación de correo electrónico, ponga el hecho en conocimiento de un abogado especializado en delitos en Internet .
4. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 197.

ÁREA ANALIZADA

A pesar de que la utilización de un sistema de firma electrónica basado en cifrado asimétrico permite proteger un documento electrónico frente a una posible falsificación con mayor eficacia que cualquier otro de los sistemas utilizados en los documentos tradicionales, también es cierto que un documento electrónico que no incluya garantías de autenticación puede ser fácilmente falsificado por cualquier usuario, aunque no disponga de conocimientos avanzados.

ACTIVIDAD PREVENTIVA

- Extreme las medidas de seguridad en el caso en que tenga que realizar una transacción de elevada cuantía a través de Internet.
- Utilice sistemas de firma electrónica si tiene que realizar una transacción de cuantía elevada.
- Exija a la otra parte una identificación completa, mediante un sistema de autenticación de la identidad.
- Compruebe que el sistema de firma electrónica utilizado cumple el principio de integridad, de manera que sean fáciles de detectar las posibles manipulaciones del documento.

ACCIONES A REALIZAR

1. En el caso de detectar indicios de una posible estafa, ponga el hecho en conocimiento de un abogado especializado en delitos en Internet.
2. Denunciarlo mediante correo electrónico en la Sección Central de Delitos en Tecnologías de la Información de la Ertzantza: scdti@utap.ej-gv.es.

LEGISLACIÓN APLICABLE

.- Código Penal: Artículo 395 y Artículo 400.

4. APÉNDICE LEGISLATIVO

CÓDIGO PENAL

■ *Artículo 197.*

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se 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 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

■ *Artículo 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.

■ *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.

■ *Artículo 264.*

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriere alguno de los supuestos siguientes:

- 1.º Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
- 2.º Que se cause por cualquier medio infección o contagio de ganado.
- 3.º Que se empleen sustancias venenosas o corrosivas.
- 4.º Que afecten a bienes de dominio o uso público o comunal.
- 5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

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.

■ *Artículo 301.*

1. El que adquiera, convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito grave, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes.

Las penas se impondrán en su mitad superior cuando los bienes tengan su origen en alguno de los delitos relacionados con el tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas descritos en los artículos 368 a 372 de este Código.

2. Con las mismas penas se sancionará, según los casos, la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos, a sabiendas de que proceden de alguno de los delitos expresados en el apartado anterior o de un acto de participación en ellos.

3. Si los hechos se realizasen por imprudencia grave, la pena será de prisión de seis meses a dos años y multa del tanto al triple.

4. El culpable será igualmente castigado aunque el delito del que provinieren los bienes, o los actos penados en los apartados anteriores hubiesen sido cometidos, total o parcialmente, en el extranjero.

■ *Artículo 390.*

1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad:

- 1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.
- 2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.
- 3.º Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho.
- 4.º Faltando a la verdad en la narración de los hechos.

2. Será castigado con las mismas penas a las señaladas en el apartado anterior el responsable de cualquier confesión religiosa que incurra en alguna de las conductas descritas en los números anteriores, respecto de actos y documentos que puedan producir efecto en el estado de las personas o en el orden civil.

■ *Artículo 395.*

El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años.

■ *Artículo 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.

CÓDIGO CIVIL

■ *Artículo 1.101*

Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas.

■ *Artículo 1.102*

La responsabilidad procedente del dolo es exigible en todas las obligaciones. La renuncia de la acción para hacerla efectiva es nula.

■ *Artículo 1.103*

La responsabilidad que proceda de negligencia es igualmente exigible en el cumplimiento de toda clase de obligaciones; pero podrá moderarse por los Tribunales según los casos.

■ *Artículo 1.104*

La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar.

Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se exigirá la que correspondería a un buen padre de familia.

■ *Artículo 1.105*

Fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse o, que, previstos, fueran inevitables.

■ *Artículo 1.106*

La indemnización de daños y perjuicios comprende, no sólo el valor de la pérdida que hayan sufrido, sino también el de la ganancia que haya dejado de obtener el acreedor, salvas las disposiciones contenidas en los artículos siguientes.

■ *Artículo 1.902*

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

Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

(BOE n.º 176, de 24 de julio de 1984)

■ *Artículo 11.*

1. El régimen de comprobación, reclamación, garantía y posibilidad de renuncia o devolución que se establezca en los contratos, deberá permitir que el consumidor o usuario se asegure de la naturaleza, características, condiciones y utilidad o finalidad del producto o servicio; pueda reclamar con eficacia en caso de error, defecto o deterioro; pueda hacer efectivas las garantías de calidad o nivel de prestación, y obtener la devolución equitativa del precio de mercado del producto o servicio, total o parcialmente, en caso de incumplimiento.

2. En relación con los bienes de naturaleza duradera, el productor o suministrador deberá entregar una garantía que, formalizada por escrito, expresará necesariamente:

- a) El objeto sobre el que recaiga la garantía.
- b) El garante.
- c) El titular de la garantía.
- d) Los derechos del titular de la garantía.
- e) El plazo de duración de la garantía.

3. Durante el período de vigencia de la garantía, el titular de la misma tendrá derecho como mínimo a:

- a) La reparación totalmente gratuita de los vicios o defectos originarios y de los daños y perjuicios por ellos ocasionados.
- b) En los supuestos en que la reparación efectuada no fuera satisfactoria y el objeto no revistiese las condiciones óptimas para cumplir el uso a que estuviese destinado, el titular de la garantía tendrá derecho a la sustitución del objeto adquirido por otro de idénticas características o a la devolución del precio pagado.

4. Queda prohibido incrementar los precios de los repuestos al aplicarlos en las reparaciones y cargar por mano de obra, traslado o visita cantidades superiores a los costes medios estimados en cada sector, debiendo diferenciarse en la factura los distintos conceptos. La lista de precios de los repuestos deberá estar a disposición del público.

5. En los bienes de naturaleza duradera, el consumidor o usuario tendrá derecho a un adecuado servicio técnico y a la existencia de repuestos durante un plazo determinado.

■ *Artículo 10 bis.*

1. Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente que en contra de las exigencias de la buena fe causen, en perjuicio del consumidor, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato. En todo caso se considerarán cláusulas abusivas los supuestos de estipulaciones que se relacionan en la disposición adicional de la presente Ley.

El hecho de que ciertos elementos de una cláusula o que una cláusula aislada se hayan negociado individualmente no excluirá la aplicación de este artículo al resto del contrato.

El profesional que afirme que una determinada cláusula ha sido negociada individualmente, asumirá la carga de la prueba.

El carácter abusivo de una cláusula se apreciará teniendo en cuenta la naturaleza de los bienes o servicios objeto del contrato y considerando todas las circunstancias concurrentes en el momento de su celebración, así como todas las demás cláusulas del contrato o de otro del que éste dependa.

2. Serán nulas de pleno derecho y se tendrán por no puestas las cláusulas, condiciones y estipulaciones en las que se aprecie el carácter abusivo. La parte del contrato afectada por la nulidad se integrará con arreglo a lo dispuesto por el artículo 1258 del Código Civil. A estos efectos, el Juez que declara la nulidad de dichas cláusulas integrará el contrato y dispondrá de facultades moderadoras respecto de los derechos y obligaciones de las partes, cuando subsista el contrato, y de las consecuencias de su ineficacia en caso de perjuicio apreciable para el consumidor o usuario. Sólo cuando las cláusulas subsistentes determinen una situación no equitativa en la posición de las partes que no pueda ser subsanada podrá declarar la ineficacia del contrato.

3. Las normas de protección de los consumidores frente a las cláusulas abusivas serán aplicables, cualquiera que sea la Ley que las partes hayan elegido para regir el contrato, en los términos previstos en el artículo 5 del Convenio de Roma de 1980, sobre la Ley aplicable a las obligaciones contractuales”.

Disposición Adicional Primera

A los efectos previstos en el artículo 10 bis, tendrán el carácter de abusivas al menos las cláusulas o estipulaciones siguientes:

I. Vinculación del contrato a la voluntad del profesional.

1.^a Las cláusulas que reserven al profesional que contrata con el consumidor un plazo excesivamente largo o insuficientemente determinado para aceptar o rechazar una oferta contractual o satisfacer la prestación debida, así como las que prevean la prórroga automática de un contrato de duración determinada si el consumidor no se manifiesta en contra, fijando una fecha límite que no permita de manera efectiva al consumidor manifestar su voluntad de no prorrogarlo.

2.^a La reserva a favor del profesional de facultades de interpretación o modificación unilateral del contrato sin motivos válidos especificados en el mismo, así como la de resolver anticipadamente un contrato con plazo determinado si al consumidor no se le reconoce la misma facultad o la de resolver en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable un contrato por tiempo indefinido, salvo por incumplimiento del contrato o por motivos graves que alteren las circunstancias que motivaron la celebración del mismo.

En los contratos referidos a servicios financieros lo establecido en el párrafo anterior se entenderá sin perjuicio de las cláusulas por las que el prestador de servicios se reserve

la facultad de modificar sin previo aviso el tipo de interés adeudado por el consumidor o al consumidor, así como el importe de otros gastos relacionados con los servicios financieros, cuando aquéllos se encuentren adaptados a un índice, siempre que se trate de índices legales y se describa el modo de variación del tipo, o en otros casos de razón válida, a condición de que el profesional esté obligado a informar de ello en el más breve plazo a los otros contratantes y éstos puedan resolver inmediatamente el contrato. Igualmente podrán modificarse unilateralmente las condiciones de un contrato de duración indeterminada, siempre que el prestador de servicios financieros esté obligado a informar al consumidor con antelación razonable y éste tenga la facultad de resolver el contrato, o, en su caso, rescindir unilateralmente, sin previo aviso en el supuesto de razón válida, a condición de que el profesional informe de ello inmediatamente a los demás contratantes.

3.^a La vinculación incondicionada del consumidor al contrato aun cuando el profesional no hubiera cumplido con sus obligaciones, o la imposición de una indemnización desproporcionadamente alta, al consumidor que no cumpla sus obligaciones.

4.^a La supeditación a una condición cuya realización dependa únicamente de la voluntad del profesional para el cumplimiento de las prestaciones, cuando al consumidor se le haya exigido un compromiso firme.

5.^a La consignación de fechas de entrega meramente indicativas condicionadas a la voluntad del profesional.

6.^a La exclusión o limitación de la obligación del profesional de respetar los acuerdos o compromisos adquiridos por sus mandatarios o representantes o supeditar sus compromisos al cumplimiento de determinadas formalidades.

7.^a La estipulación del precio en el momento de la entrega del bien o servicio, o la facultad del profesional para aumentar el precio final sobre el convenido, sin que en ambos casos existan razones objetivas o sin reconocer al consumidor el derecho a rescindir el contrato si el precio final resultare muy superior al inicialmente estipulado.

Lo establecido en el párrafo anterior se entenderá sin perjuicio de la adaptación de precios a un índice, siempre que sean legales y que en ellos se describa explícitamente el modo de variación del precio.

8.^a La concesión al profesional del derecho a determinar si el bien o servicio se ajusta a lo estipulado en el contrato.

II. Privación de derechos básicos del consumidor.

9.^a La exclusión o limitación de forma inadecuada de los derechos legales del consumidor por incumplimiento total o parcial o cumplimiento defectuoso del profesional.

En particular las cláusulas que modifiquen, en perjuicio del consumidor, las normas legales sobre vicios ocultos, salvo que se limiten a reemplazar la obligación de saneamiento por la de reparación o sustitución de la cosa objeto del contrato, siempre que no conlleve dicha reparación o sustitución gasto alguno para el consumidor y no excluyan o limiten los derechos de éste a la indemnización de los daños y perjuicios ocasionados por los vicios y al saneamiento conforme a las normas legales en el caso de que la reparación o sustitución no fueran posibles o resultasen insatisfactorias.

10. La exclusión o limitación de responsabilidad del profesional en el cumplimiento del contrato, por los daños o por la muerte o lesiones causados al consumidor debidos a una acción u omisión por parte de aquél, o la liberación de responsabilidad por cesión del contrato a tercero, sin consentimiento del deudor, si puede engendrar merma de las garantías de éste.

11. La privación o restricción al consumidor de las facultades de compensación de créditos, así como de la de retención o consignación.

12. La limitación o exclusión de forma inadecuada de la facultad del consumidor de resolver el contrato por incumplimiento del profesional.

13. La imposición de renuncias a la entrega de documento acreditativo de la operación.

14. La imposición de renuncias o limitación de los derechos del consumidor.

III. Falta de reciprocidad.

15. La imposición de obligaciones al consumidor para el cumplimiento de todos sus deberes y contraprestaciones, aun cuando el profesional no hubiere cumplido los suyos.

16. La retención de cantidades abonadas por el consumidor por renuncia, sin contemplar la indemnización por una cantidad equivalente si renuncia el profesional.

17. La autorización al profesional para rescindir el contrato discrecionalmente, si al consumidor no se le reconoce la misma facultad, o la posibilidad de que aquél se quede con las cantidades abonadas en concepto de prestaciones aún no efectuadas cuando sea él mismo quien rescinda el contrato.

IV. Sobre garantías.

18. La imposición de garantías desproporcionadas al riesgo asumido. Se presumirá que no existe desproporción en los contratos de financiación o de garantías pactadas por entidades financieras que se ajusten a su normativa específica.

19. La imposición de la carga de la prueba en perjuicio del consumidor en los casos en que debería corresponder a la otra parte contratante.

V. Otras.

20. Las declaraciones de recepción o conformidad sobre hechos ficticios, y las declaraciones de adhesión del consumidor a cláusulas de las cuales no ha tenido la oportunidad de tomar conocimiento real antes de la celebración del contrato.

21. La transmisión al consumidor de las consecuencias económicas de errores administrativos o de gestión que no le sean imputables.

22. La imposición al consumidor de los gastos de documentación y tramitación que por Ley imperativa corresponda al profesional. En particular, en la primera venta de viviendas, la estipulación de que el comprador ha de cargar con los gastos derivados de la preparación de la titulación que por su naturaleza correspondan al vendedor (obra nueva, propiedad horizontal, hipotecas para financiar su construcción o su división y cancelación).

23. La imposición al consumidor de bienes y servicios complementarios o accesorios no solicitados.

24. Los incrementos de precio por servicios accesorios, financiación, aplazamientos, recargos, indemnización o penalizaciones que no correspondan a prestaciones adicionales susceptibles de ser aceptados o rechazados en cada caso expresados con la debida claridad o separación.

25. La negativa expresa al cumplimiento de las obligaciones o prestaciones propias del productor o suministrador, con reenvío automático a procedimientos administrativos o judiciales de reclamación.

26. La sumisión a arbitrajes distintos del de consumo, salvo que se trate de órganos de arbitraje institucionales creados por normas legales para un sector o un supuesto específico.

27. La previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si fuera inmueble, así como los de renuncia o transacción respecto al derecho del consumidor a la elección de fedatario competente según la Ley para autorizar el documento público en que inicial o ulteriormente haya de formalizarse el contrato.

28. La sumisión del contrato a un Derecho extranjero con respecto al lugar donde el consumidor emita su declaración negocial o donde el profesional desarrolle la actividad dirigida a la promoción de contratos de igual o similar naturaleza.

29. La imposición de condiciones de crédito que para los descubiertos en cuenta corriente superen los límites que se contienen en el artículo 19.4 de la Ley 7/1995, de 23 de marzo de Crédito al Consumo.

Las cláusulas abusivas referidas a la modificación unilateral de los contratos y resolución anticipada de los de duración indefinida, y al incremento del precio de bienes y servicios, no se aplicarán a los contratos relativos a valores, con independencia de su forma de representación, instrumentos financieros y otros productos y servicios cuyo precio esté vinculado a una cotización, índice bursátil, o un tipo del mercado financiero que el profesional no controle, ni a los contratos de compraventa de divisas, cheques de viaje, o giros postales internacionales en divisas.

Se entenderá por profesional, a los efectos de esta disposición adicional, la persona física o jurídica que actúa dentro de su actividad profesional, ya sea pública o privada”.

Ley 34/1988, de 11 de noviembre, General de Publicidad

(BOE n.º 274, de 15 de noviembre de 1988)

■ *Artículo 4.*

Es engañosa la publicidad que de cualquier manera, incluida su presentación, induce o puede inducir a errores a sus destinatarios, pudiendo afectar a su comportamiento económico, o perjudicar o ser capaz de perjudicar a un competidor.

Es asimismo engañosa la publicidad que silencie datos fundamentales de los bienes, actividades o servicios cuando dicha omisión induzca a un error de los destinatarios.

■ *Artículo 5.*

Para determinar si una publicidad es engañosa, se tendrá en cuenta todos sus elementos y principalmente sus indicaciones concernientes a:

1. Las características de los bienes, actividades o servicios, tales como:
 - a) Origen de procedencia geográfica o comercial, naturaleza, composición, destino, finalidad, idoneidad, disponibilidad y novedad.
 - b) Calidad, cantidad, categoría, especificaciones y denominación.
 - c) Modo y fecha de fabricación, suministro o presentación.
 - d) Resultados que pueden esperarse de su utilización.
 - e) Resultados y características esenciales de los ensayos o controles de los bienes o servicios.
 - f) Nocividad o peligrosidad.
2. Precio completo o presupuesto o modo de fijación del mismo.
3. Condiciones jurídicas y económicas de adquisición, utilización y entrega de los bienes o de la prestación de los servicios.
4. Motivo de la oferta.
5. Naturaleza, cualificaciones y derechos del anunciante, especialmente en lo relativo a:
 - a) Identidad, patrimonio y cualificaciones profesionales.
 - b) Derechos de propiedad industrial o intelectual.
 - c) Premios o distinciones recibidas.
6. Servicios post-venta.

Ley 7/1996, de 17 de enero, de Ordenación del Comercio Minorista

(BOE n.º 42, de 17 de febrero de 1996)

■ *Artículo 12. Garantía y servicio postventa.*

1. El vendedor responderá de la calidad de los artículos vendidos en la forma determinada en los Códigos Civil y Mercantil, así como en la Ley General para la Defensa de los Consumidores y Usuarios y normas concordantes y complementarias.

2. El plazo mínimo de la garantía, en el caso de bienes de carácter duradero, será de seis meses a contar desde la fecha de recepción del artículo que se trate, salvo cuando la naturaleza del mismo lo impidiera y sin perjuicio de las disposiciones legales o reglamentarias específicas para bienes o servicios concretos.

3. El productor, o, en su defecto, el importador, garantizará, en todo caso, frente a los compradores, la existencia de un adecuado servicio técnico para los bienes de carácter duradero que fabrica o importa así como el suministro de piezas de repuesto durante un plazo mínimo de cinco años a contar desde la fecha en que el producto deje de fabricarse.

Para facilitar el ejercicio de este derecho el vendedor en el momento de la entrega del bien extenderá por cuenta del fabricante o importador, o, en su defecto, en nombre propio, el documento de garantía y le proporcionará las instrucciones suficientes para el correcto uso e instalación del artículo así como para la formulación de las reclamaciones pertinentes.

4. La acción o derecho de recuperación de los géneros entregados por el consumidor o usuario al comerciante para su reparación prescribirá a los tres años a partir del momento de la entrega. Reglamentariamente se establecerán los datos que deberá hacer constar el comerciante en el momento en que se le entrega un objeto para su reparación y las formas en que podrá acreditarse la mencionada entrega.

■ *Artículo 40. Contenido de las propuestas.*

La oferta de venta a distancia deberá incluir, al menos, los siguientes extremos:

- a) Identidad del proveedor.
- b) Características especiales del producto.
- c) Precio y, en su caso, debidamente separados, los gastos del transporte.
- d) Forma de pago y modalidades de entrega o de ejecución.
- e) Plazo de validez de la oferta.

■ *Artículo 43. Plazo de ejecución y pago.*

1. De no indicarse en la oferta el plazo de ejecución del pedido, éste deberá cumplimentarse dentro de los treinta días siguientes al de su recepción por el vendedor.

2. Sólo podrá exigirse el pago antes de la entrega del producto cuando se trate de un pedido que se haya elaborado con algún elemento diferenciador para un cliente específico y a solicitud del mismo.

■ *Artículo 44. Derecho de desistimiento.*

1. El comprador podrá desistir libremente del contrato dentro del plazo de siete días contados desde la fecha de recepción del producto. En el caso de que la adquisición del producto se efectuase mediante un acuerdo de crédito, el desistimiento del contrato principal implicará la resolución de aquél.

2. El ejercicio del derecho o desistimiento no estará sujeto a formalidad alguna, bastando que se acredite, en cualquier forma admitida en Derecho.

3. El derecho de desistimiento del comprador no puede implicar la imposición de penalidad alguna, si bien, el comprador deberá satisfacer los gastos directos de devolución y, en su caso, indemnizar los desperfectos del objeto de la compra.

■ *Artículo 45. Excepciones al derecho de desistimiento.*

Lo dispuesto en el artículo anterior no será de aplicación a los siguientes supuestos:

1) A las transacciones de valores mobiliarios y otros productos cuyo precio esté sujeto a fluctuaciones de un mercado no controlado por el proveedor.

2) A los contratos celebrados con intervención de fedatario público.

3) Tampoco se extenderá el derecho de desistimiento, salvo pacto en contrario, a las ventas de objetos que puedan ser reproducidos o copiados con carácter inmediato, que se destinen a la higiene corporal o que, en razón de su naturaleza, no puedan ser devueltos.

■ *Artículo 46. Pago mediante tarjeta de crédito.*

1. Cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo.

En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad.

2. Sin embargo, si la compra hubiese sido efectivamente realizada por el titular de la tarjeta y, por lo tanto, hubiese exigido indebidamente la anulación del correspondiente cargo, aquél quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

(BOE n.º 298, de 14 de diciembre de 1999)

■ *Artículo 4. Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

■ *Artículo 5. Derecho a información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o de organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

■ *Artículo 6. Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del

tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

■ *Artículo 11. Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

- a) Cuando la cesión está autorizada en una ley.
- b) Cuando se trate de datos recogidos de fuentes accesibles al público.
- c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente concesión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.
- f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilita al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

■ *Artículo 15. Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

■ *Artículo 16. Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificadas o canceladas hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

■ *Artículo 27. Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Ley 7/1998, de 13 de abril, de Condiciones Generales de Contratación

(BOE n.º 89, de 14 de abril de 1998)

■ *Artículo 5. Requisitos de incorporación.*

1. Las condiciones generales pasarán a formar parte del contrato cuando se acepte por el adherente su incorporación al mismo y sea firmado por todos los contratantes. Todo contrato deberá hacer referencia a las condiciones generales incorporadas.

No podrá entenderse que ha habido aceptación de la incorporación de las condiciones generales al contrato cuando el predisponente no haya informado expresamente al adherente acerca de su existencia y no le haya facilitado un ejemplar de las mismas.

2. Cuando el contrato no deba formalizarse por escrito y el predisponente entregue un resguardo justificativo de la contraprestación recibida, bastará con que el predisponente anuncie las condiciones generales en un lugar visible dentro del lugar en el que se celebra el negocio, que las inserte en la documentación del contrato que acompaña su celebración; o que, de cualquier otra forma, garantice al adherente una posibilidad efectiva de conocer su existencia y contenido en el momento de la celebración.

3. En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.

4. La redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez.

Real Decreto-Ley 14/1999, de 17 de septiembre de 1999. Firma Electrónica

(BOE n.º 224, de 18 de septiembre de 1999)

■ *Artículo 3. Efectos jurídicos de la firma electrónica.*

1. La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el

dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

2. A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

Ley 3/1991, de 10 de enero, de Competencia Desleal

(BOE n.º 10, de 11 de enero de 1991)

■ *Artículo 6. Actos de confusión.*

Se considera desleal todo comportamiento que resulte idóneo para crear confusión con la actividad, las prestaciones o el establecimiento ajenos. El riesgo de asociación por parte de los consumidores respecto de la procedencia de la prestación es suficiente para fundamentar la deslealtad de una práctica.

Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13-4-1998, de condiciones generales de la contratación.

(BOE n.º 313, de 31 de diciembre de 1999)

■ *Artículo 1. Ambito de aplicación.*

1. El presente Real Decreto se aplicará a los contratos a distancia, o sin presencia física simultánea de los contratantes, realizados por vía telefónica, electrónica o telemática, que contengan condiciones generales de la contratación, entendiéndose por tales las definidas por la Ley 7/1998, de 13 de abril, y se entiende sin perjuicio de la aplicación de las normas vigentes en materia de firma electrónica contenidas en el Real Decreto-ley 14/1999, de 17 de diciembre.

2. El presente Real Decreto no será aplicable a los contratos administrativos, los contratos de trabajo, los de constitución de sociedades, los que regulan relaciones familiares y los contratos sucesorios, como tampoco a los contratos relativos a condiciones generales, que reflejen las disposiciones a los principios de los Convenios internacionales en que el Reino de España sea parte, y los que se refieren a condiciones reguladas específicamente por una disposición legal o administrativa de carácter general, que sean de aplicación obligatoria para los contratantes.

3. Igualmente quedan excluidos los contratos referidos a servicios financieros consistentes en servicios de inversión, instituciones de inversión colectiva, seguro y reaseguro, bancarios o prestados por entidades sujetas a supervisión prudencial, relativos a fondos de pensiones y a operaciones a plazo y de opción, los celebrados mediante máquinas o locales automáticos, en subasta y los relativos a la construcción y venta de bienes inmuebles y demás relativos a derechos reales sobre los mismos, así como los de arrendamiento de bienes inmuebles regulados por leyes especiales, excepto los arrendamientos de temporada, a los cuales será de aplicación la presente norma.

No obstante, en estos supuestos, deberá quedar constancia documental de la contratación efectuada, ya sea en forma escrita o en registros magnéticos o informáticos, de acuerdo con la normativa específica aplicable en cada caso. A falta de ésta, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.

4. Las normas contenidas en este Real Decreto son de aplicación siempre que la adhesión a las condiciones generales se haya efectuado en España, cualquiera que sea la ley aplicable al contrato.

■ *Artículo 2. Deber de información previa.*

Previamente a la celebración del contrato y con la antelación necesaria, como mínimo en los tres días naturales anteriores a aquélla, el predisponente deberá facilitar al adherente, de modo veraz, eficaz y completo, información sobre todas y cada una de las cláusulas del contrato y remitirle, por cualquier medio adecuado a la técnica de comunicación a distancia utilizada, el texto completo de las condiciones generales.

■ *Artículo 3. Confirmación documental de la contratación efectuada.*

1. Celebrado el contrato, el predisponente deberá enviar al adherente inmediatamente y, a más tardar, en el momento de la entrega de la cosa o comienzo de la ejecución del contrato, justificación por escrito o, a propuesta del mismo, en cualquier otro soporte duradero adecuado al medio de comunicación empleado y en su propio idioma o en el utilizado por el predisponente para hacer la oferta, relativa a la contratación efectuada donde deberán constar todos los términos de la misma. A los efectos de lo indicado en este apartado, el predisponente deberá indicar en la información previa a que se refiere el artículo anterior los distintos tipos de soportes entre los que podrá elegir el adherente como medio de recepción de la justificación de la contratación efectuada.

2. Lo dispuesto en el apartado 1 no será aplicable a los contratos relativos a servicios de tracto único que se ejecutan mediante el empleo de técnicas de comunicación a distancia y cuya facturación sea efectuada por un operador de tales técnicas de comunicación, y sin perjuicio de informar en todo caso al adherente de la dirección del establecimiento del proveedor donde pueda presentar sus reclamaciones y del coste específico y separado de la comunicación y del servicio.

3. Se entiende por soporte duradero cualquier instrumento que permita al consumidor conservar sus informaciones sin que se vea obligado a realizar por sí mismo su almacenamiento, en particular los disquetes informáticos y el disco duro del ordenador del consumidor que almacena los mensajes del correo electrónico.

■ *Artículo 4. Derecho resolución.*

1. Cumplidas las obligaciones a que se refieren los artículos 2 y 3, el adherente dispondrá de un plazo de siete días hábiles, según el calendario oficial de su lugar de residencia habitual, para resolver el contrato sin incurrir en penalización ni gasto alguno, incluidos los correspondientes a la devolución del bien.

El ejercicio del derecho a que se refiere este apartado no estará sujeto a formalidad alguna, bastando que se acredite, en cualquier forma admitida en derecho.

2. El plazo para el ejercicio del derecho a que se refiere el párrafo anterior se computará, en el caso de que el contrato tenga por objeto la entrega de bienes, a partir de su recepción por el adherente, y en los casos de prestaciones de servicios a partir del día de celebración del contrato.

3. Si la información sobre las condiciones generales o la confirmación documental tiene lugar con posterioridad a la entrega de los bienes o a la celebración del contrato, respectivamente, el plazo se computará desde que tales obligaciones queden totalmente cumplidas. En caso de cumplimiento defectuoso o incompleto de la obligación de remitir justificación documental de los términos del contrato a que se refiere el artículo anterior, la acción de resolución no caducará hasta transcurridos tres meses computados en la forma establecida en el apartado anterior.

4. Ejercitado el derecho de resolución el predisponente estará obligado a devolver las cantidades recibidas sin retención alguna inmediatamente y nunca después de treinta días.

5. Queda excluido el derecho de resolución en aquellos casos en que por la naturaleza del contenido de las prestaciones sea imposible llevarlo a cabo, sin perjuicio de la reclamación de los daños y perjuicios sufridos.

■ *Artículo 5. Atribución de la carga de la prueba.*

1. La carga de la prueba sobre la existencia y contenido de la información previa de las cláusulas del contrato; de la entrega de las condiciones generales; de la justificación documental de la contratación una vez efectuada; de la renuncia expresa al derecho de resolución; así como de la correspondencia entre la información, entrega y justificación documental y al momento de sus respectivos envíos, corresponde al predisponente.

2. A estos efectos, y sin perjuicio de cualquier otro medio de prueba admitido en derecho, cualquier documento que contenga la citada información aun cuando no se haya extendido en soporte papel, como las cintas de grabaciones sonoras, los disquetes y, en particular, los documentos electrónicos y telemáticos, siempre que quede garantizada su autenticidad, la identificación fiable de los manifestantes, su integridad, la no alteración del contenido de lo manifestado, así como el momento de su emisión y recepción, será aceptada en su caso, como medio de prueba en los términos resultantes de la legislación aplicable.

Para ello, en los casos de contratación electrónica, deberá utilizarse una firma electrónica avanzada que atribuya a los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita, conforme a lo dispuesto en el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica. En estos casos, al documento electrónico se acompañará una consignación de fecha y hora de remisión y recepción, en su caso.

OTRAS REFERENCIAS

Ley 36/1988, de 5 de diciembre. Régimen Jurídico del Arbitraje. (BOE n.º 293, de 7 de diciembre de 1988).

Real Decreto 636/1993, de 3 de mayo, por el que se regula el Sistema Arbitral de Consumo. (BOE n.º 121, de 21 de mayo de 1993).

Sentencia del Tribunal Supremo de 3 de noviembre de 1997 (Firma Electrónica). (Marginal Aranzadi RJ 1997\8252).

Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia. (DOCE n.º L 144, de 4 de junio de 1997).

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico, en el Mercado Interior (Directiva sobre el Comercio Electrónico) (DOCE n.º L 178, de 17 de julio de 2000).

<http://www.aece.org/legislacion/DirectivaCE.pdf>

Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad (AAP): <http://www.aap.es>

Código Ético de la Asociación Española de Comercio Electrónico (AECE):
<http://www.aece.org>:

Recomendaciones a los Usuarios de Internet de la Agencia de Protección de Datos (APD):
<http://www.agenciaprotecciondatos.org>

5. GLOSARIO DE TÉRMINOS

ALGORITMO	Fórmula matemática o secuencia de normas ordenadas para solucionar un problema en un número determinado de pasos.
ALGORITMO CRIPTOGRÁFICO	Serie de normas que especifican el procedimiento requerido para cifrar y descifrar datos.
ANCHO DE BANDA	Forma de medir el volumen de información que puede ser transferida a través de un segmento de la red.
APPLETS	Pequeños programas de Java que permiten ser ejecutados dentro de un navegador y desde cualquier sistema operativo.
ASIMÉTRICO	Sistema de cifrado que utiliza una clave para cifrar y otra clave distinta para descifrar.
ASÍNCRONO	Suceso que ocurre de forma irregular o impredecible.
AUTENTIFICACIÓN	Proceso mediante el cual se confirma la identidad de los usuarios que intervienen en una transacción o el origen de los datos.
BASE DE DATOS	Colección de datos que tienen una estructura en común.
BIT	La unidad más pequeña de información que un ordenador puede procesar.
BROWSER (NAVEGADOR)	Programa que utiliza el usuario para visualizar los contenidos de una página web en Internet.
BUSCADOR	Programa accesible de forma remota que permite búsquedas de información en Internet mediante la introducción de palabras clave.
BUZÓN DE CORREO ELECTRÓNICO	Sección de un servidor destinada a albergar los mensajes entrantes y salientes de un usuario de correo electrónico.
CACHÉ	Sección reservada del disco duro de un sistema informático o de la unidad central de proceso que actúa como memoria temporal para los documentos más recientes o más frecuentemente consultados.
CÁMARA DE COMPENSACIÓN	Sistema que ofrece la posibilidad de almacenar mensajes y distribuirlos en nombre de otras organizaciones.
CATÁLOGO ELECTRÓNICO	Base de datos accesible a través de Internet que contiene la descripción de diversos productos, imágenes, precios, etc.
CERTIFICADO	Archivo electrónico que asocia una clave criptográfica a un usuario determinado e incluye la firma digital de una entidad de certificación y los demás elementos necesarios para la autenticación.
CIFRADO DE LA INFORMACIÓN	Proceso de transformación de los datos a un formato ininteligible de manera que los datos originales solo pueden ser recuperados mediante un proceso de descifrado que utilice el mismo algoritmo. En los casos en los que se

	utiliza una clave de cifrado igual a la clave de descifrado estamos ante un sistema de clave simétrica, cuando ambas claves son distintas estaremos ante un sistema de clave asimétrica.
CLAVE PRIVADA	Una de las dos claves utilizadas en sistemas de claves asimétrico que solo es conocida por su propietario.
CLAVE PÚBLICA	Una de las dos claves utilizadas en un sistema de cifrado asimétrico y que es accesible al público.
CLIENTE-SERVIDOR	Configuración de sistemas informáticos que permite el acceso múltiple de terminales o programas cliente a los datos almacenados en las bases de datos de un servidor.
CÓDIGO FUENTE	Lenguaje de alto nivel en el que están escritos los programas antes de pasarlos a formato ejecutable. En las páginas web, el código fuente está en lenguaje HTML.
CABALLO DE TROYA	Programa o fichero que se introduce en un sistema con el fin de permitir el acceso no autorizado en posteriores ocasiones.
COMERCIO ELECTRÓNICO	Término general referido al comercio mediante uso de aplicaciones informáticas a través de las redes de telecomunicaciones.
CONFIRMACIÓN	Notificación que una transmisión ha sido recibida correctamente por el destinatario de la misma.
CORTAFUEGOS	Una combinación de hardware y software que separa o filtra la comunicación entre dos o más elementos de una red con el fin de garantizar la seguridad de los datos y controlar los accesos.
DINERO ELECTRÓNICO	Se aplica generalmente al dinero que se utiliza exclusivamente para pagos a través de redes telemáticas.
DOWNLOAD	Proceso de descarga de un fichero desde un servidor al ordenador del usuario.
EDI (Electronic Data Interchange)	Intercambio electrónico de datos. No se destina al comercio de consumo, sino al comercio entre empresas.
ENCRIPCIÓN	Proceso de transformación de los datos a un formato ininteligible de manera que los datos originales solo pueden ser recuperados mediante un proceso de descifrado que utilice el mismo algoritmo. En los casos en los que se utiliza una clave de cifrado igual a la clave de descifrado estamos ante un sistema de clave simétrica, cuando ambas claves son distintas estaremos ante un sistema de clave asimétrica.
ENLACE HIPERTEXTUAL	Referencia a otros contenidos ubicados en el mismo servidor o en otro servidor de la red que convierte el texto ordinario en hipertexto.
ENTIDAD DE CERTIFICACIÓN	Entidad que merece la confianza tanto de los comerciantes como de los usuarios para emitir certificados que identifiquen a las partes de una transacción.
FIREWALL	Una combinación de hardware y software que separa o filtra la comunicación entre dos o más elementos de una red con el fin de garantizar la seguridad de los datos y controlar los accesos.

FIRMA DIGITAL	Datos cifrados que pertenecen a las partes de una transacción segura y cuya finalidad es demostrar la autenticidad y la integridad de las transacciones.
FTP	Protocolo que permite la transferencia de ficheros entre un servidor y sus usuarios.
GATEWAY	Conexión entre dos redes distintas que permite que los datos de una puedan ser encaminados hacia la otra.
GIF	Formato de compresión de imágenes utilizado para visualizar fotografías a través de páginas web.
HASH	Función informática que reduce un importante número de bits a un número más pequeño de manera que la disposición de todos los bits originales influya en el resultado final. Se utiliza en las firmas digitales y en los sistemas de cifrado de la información.
HIPERTEXTO	Texto que contiene un enlace a otros contenidos del mismo servidor o de otros servidores conectados a Internet.
HOME PAGE	Página principal de un web.
HOST	Ordenador conectado a una red que suministra servicios o contenidos a otros ordenadores llamados terminales.
HTML	Lenguaje utilizado para desarrollar las páginas web que se basa en el hipertexto.
IDENTIFICADOR	Cadena de caracteres utilizadas para identificar a una persona en combinación con una clave secreta o password.
INTEGRIDAD DE LOS DATOS	Principio que rige en las transacciones seguras mediante el cual los datos transmitidos a través de una transacción están libres de errores y permanecen inalterados.
INTRANET	Red privada que utiliza los mismos protocolos que la red Internet.
IRC	Sistema de comunicación por Internet que permite el diálogo en tiempo real entre varios usuarios.
JPG	Formato de compresión de imágenes utilizado para visualizar fotografías a través de páginas web.
LINK	Referencia a otros contenidos ubicados en el mismo servidor o en otro servidor de la red que convierte el texto ordinario en hipertexto.
MODEM	Dispositivo que convierte la información digital de un ordenador a una serie de tonos y sonidos que permiten su transmisión a través de líneas telefónicas en una señal portadora analógica y viceversa.
MOTOR DE BÚSQUEDA	Programa accesible de forma remota que permite búsquedas de información en Internet mediante la introducción de palabras clave.
MP3	Formato de compresión utilizado para la venta de música a través de Internet.
NAVEGADOR	Programa que utiliza el usuario para visualizar los contenidos de una página web en Internet.

NO REPUDIO	Principio inherente a una transacción segura que impide a las partes negar su participación en la misma.
NOMBRE DE DOMINIO	Denominación alfanumérica que se utiliza como nemotécnico para referirse a una dirección IP en Internet.
ON - LINE	Propiedad de cualquier sistema o servicio accesible a través de un sistema telemático.
OPT-IN:	Sistema aplicado al marketing directo mediante el cual sólo las personas que se han dado de alta voluntariamente en una lista pueden recibir correo comercial no solicitado.
OPT-OUT	Sistema aplicado al marketing directo mediante el cual las personas que figuran en una lista llamada "Robinson" deben ser excluidas de cualquier base de datos utilizada para el envío de correo comercial.
PASARELA	Conexión entre dos redes distintas que permite que los datos de una puedan ser encaminados hacia la otra.
PIN	Código numérico o alfanumérico, generalmente de cuatro cifras que se utiliza como contraseña para conseguir el acceso a un sistema.
PSI	Proveedor de servicios de Internet.
RSA	Algoritmo de cifrado asimétrico creado por Rivest, Shamir y Adleman.
SET	Protocolo de seguridad diseñado para las transacciones en Internet, que permite comprobar la identidad de las partes intervinientes.
SPAM	Envío masivo de correo electrónico no solicitado y con contenido publicitario a una pluralidad de usuarios de Internet.
TARJETA INTELIGENTE	Tarjeta de plástico similar a una tarjeta de crédito que contiene un circuito integrado en el que puede almacenarse información, certificados, programas y dinero electrónico.
TRANSFERENCIA ELECTRÓNICA DE FONDOS	Comunicación electrónica que permite ordenar a una entidad financiera el traspaso de cantidades determinadas de dinero de una cuenta correspondiente al titular a otra cuenta correspondiente del mismo titular o de otros.
URL	Dirección de Internet.
VALIDACIÓN	Proceso utilizado para comprobar el cumplimiento de los requisitos de autenticidad de un mensaje o una transacción.
WORLD WIDE WEB	Sistema utilizado en Internet para almacenar y distribuir documentos basado en la utilización del hipertexto y programas navegadores.

6. LINKS

Departamento de Industria, Comercio y Turismo.

Dirección de Consumo

Centro Europeo del Consumidor

E-mail: cec@ej.gv.es

<http://www.euskadi.net/consumoinfo>

Agencia de Protección de Datos

<http://www.agenciaprotecciondatos.org>

Asociación de Autocontrol de la Publicidad

<http://www.aap.es>

Asociación Española de Comercio Electrónico

<http://www.aece.org>

Federación de Comercio Electrónico y Marketing Directo

(Servicio de Listas Robinson)

<http://www.fecemd.org/>

Internet Contract-Soft

<http://www.onnet.es>

