Ciencias Económicas 28-No. 1: 2010 / 117-139 / ISSN: 0252-9521

LOS CÓDIGOS DE CONDUCTA COMO SOLUCIÓN FRENTE A LA FALTA DE SEGURIDAD EN MATERIA DE COMERCIO ELECTRÓNICO

David López Jiménez[1]
Francisco José Martínez López[2]

ÍNDICE

Resumen 117
Summary 118
1. Introducción 118
2. Alcance de la seguridad electrónica en función de la etapa contractual 119
2.1. Relación precontractual 120
2.2. Perfección del contrato: pago de la transacción 121
3. Virtualidad de la autorregulación del comercio electrónico 127
4. Los códigos de conducta como paradigma de referencia. 128
4.1. Concepto 128
4.2. Contenido en materia de seguridad 129
4.3. Eficacia 132
5. Conclusiones 134
6. Bibliografía 135

RESUMEN

El comercio electrónico adolece de una importante sensación de desconfianza por parte de sus usuarios. Tal impresión se debe, en gran medida, a la deficiente seguridad que en tal medio existe. Sin embargo, para hacer frente a tal inconveniente, se han ideado los denominados códigos de conducta. Tales instrumentos se erigen en verdaderos paradigmas de referencia (sobre todo en el ámbito de la seguridad) para el colectivo empresarial que desarrolla actividades susceptibles de ser conceptualizadas como de comercio electrónico.

PALABRAS CLAVE: CÓDIGOS DE CONDUCTA, COMERCIO ELECTRÓNICO, CONFIANZA"; PAGO ELECTRÓNICO, SEGURIDAD.

1 Doctor, Becario de investigación del Ministerio de Educación y Ciencia de España. Programa FPU dlopez3@us.es

2 Catedrático, Doctor y Rector de la Universidad de Huelva (España) rector@uhu.es

SUMMARY

Electronic commerce suffers from an important feeling of mistrust from its users. Such impression is due to, in great part and in great measures, to the deficiency in security that exists in this area. However, to face such inconvenience, codes of conduct have had to be devised. These codes are erected in true paradigms of reference (mostly in the area of security) for the business collective agreement that develop activities that are susceptible of being conceptualized as electronic commerce.

KEY WORDS: CODES OF CONDUCT, ELECTRONIC COMMERCE, TRUST, ELECTRONIC PAYMENT, SECURITY.

1. INTRODUCCIÓN

La seguridad se erige como un desafío clave de alcance mundial. Las redes, paulatinamente, son más convergentes y prestan mayores servicios si bien, simultáneamente, se incrementa su vulnerabilidad siendo necesarios la creación y establecimiento de una importante política de seguridad.

Existe relativa unanimidad en que la seguridad electrónica constituye una cualidad precisa para la consolidación del comercio electrónico. Entendemos que la seguridad, en materia de contratación electrónica, debe examinarse necesariamente desde dos perspectivas. En primer término, desde un punto de vista jurídico para, posteriormente, considerar el plano técnico. Sin duda, ambos puntos de vista están estrechamente interrelacionados pues, como no podía ser de otro modo, el Derecho regula aspectos relativos a la seguridad electrónica teniendo en cuenta los aspectos técnicos que, precisamente, definen el marco regulador. Además, debemos ser conocedores de la extraordinaria rapidez con la que las novedades tecnológicas tienen lugar, sobre todo en cuestiones vinculadas con la seguridad electrónica y, en especial, los medios de pago, a las que, de una u otra forma, el Derecho tendrá que hacer frente en términos de aprobar una regulación eficaz que responda y tenga en consideración las novedades tecnológicas que, en cada momento, se susciten (Boix Palop, 2006).

Aunque la seguridad, obviamente, está fundamentalmente ligada a la implantación de medios técnicos excepcionalmente avanzados, sobre todo vinculados con los medios de pago, para el momento en el que se aplican, constituye un valor, a su vez, afín a otros no, por ello, menos significativos. Nos referimos, entre otras cuestiones, a las medidas adoptadas para garantizar la protección integral, permanente y sin fisuras de los datos de carácter personal y, naturalmente, de los pagos.

El riesgo percibido por el consumidor o usuario, vinculado indefectiblemente a la seguridad, repercute negativamente por lo que respecta a la adopción del comercio electrónico como alternativa para la compra de bienes o la contratación de servicios (González, 1999; Korgaonkar y Wolin, 1999; Bolás Alfonso, 2000; Sisodia y Wolfe, 2000; Alonso, 2001; Sánchez Bravo, 2001; Villanueva e Iniesta, 2001; Arranz y González Espasas, 2002; Barreiros Fernández, 2002; Delgado Bustos, 2002; Feliu Rey, 2002; Fernández Gómez, 2002; Kalyanam, 2002; Vilches Trasierra, 2002; Barral Viñals, 2003; Joines, Scherer y Scheufele, 2003; Madrid Parra, 2003; Plaza Penadés, 2003; Park, Lee y Ahn, 2004; Melián Alzola y Padrón Robaina, 2005; De Pablo Redondo, 2006; Fernández Rodríguez, 2006; Rufín Moreno, 2008). En este sentido, debería desarrollarse una infraestructura en virtud de la cual pudieran realizarse todas las operaciones con similares criterios de seguridad que los existentes en el mundo físico (Ribagorda Garnacho, 2008).

Debemos precisar que hemos dejado a un lado el estudio de la firma electrónica, regulada por la Ley 56/2003, de 13 de diciembre, precisamente por el hecho de que constituye un mecanismo de seguridad que, por el momento, no es objeto de uso habitual, sino más bien todo lo contrario, en el ámbito del comercio electrónico.

Sin embargo, como bien sugiere García Más (1998, 1999, 2000 y 2004), para el desarrollo integral del comercio electrónico, en aspectos tan esenciales como el de la seguridad y el de la confianza en el destinatario de los servicios, la firma electrónica en el futuro desempeñará un papel verdaderamente relevante como soporte tecnológico para dar fiabilidad en los principios de integridad del mensaje, autenticidad, confidencialidad y no repudio.

No obstante, su recurso resulta muy habitual en las relaciones de los ciudadanos con la Administración Pública. En efecto, las diversas Administraciones Públicas permiten, a través de sus respectivos sitios *Web*, realizar, haciendo uso de la firma electrónica, multitud de gestiones desde Internet, evitando engorrosos desplazamientos y largas colas, innecesarias, dicho sea de paso, en muchos casos.

A continuación nos ocuparemos de la seguridad en el comercio electrónico teniendo en consideración tanto la actividad a desarrollar como la fase o etapa de la relación contractual en la que la misma se inserte. Dicho de otro modo, no será igual, tanto desde el punto de vista técnico como jurídico, los instrumentos de garantía de la seguridad en la fase precontractual de la relación jurídica, en la que generalmente se dan a conocer por parte del potencial consumidor o usuario numerosos datos de carácter personal, que aquellos que deben implantarse en el momento de efectuar el pago de la transacción electrónica. En cualquier caso, en ambos supuestos, debe garantizarse, en todo caso, la confidencialidad de la operación y otros extremos adicionales a los que, en el siguiente apartado, nos referiremos.

Posteriormente, aludiremos a las interesantes aportaciones que, en base a la autorregulación del comercio electrónico, se han realizado en materia de seguridad electrónica. En efecto, como en el presente estudio veremos, los códigos de conducta reguladores del comercio electrónico, paradigma de los sistemas de autodisciplina, aseguran elevados niveles de seguridad para los consumidores y/o usuarios que contraten con las empresas que efectivamente se adhieran a los mismos. De tales instrumentos contractuales examinaremos su concepto, contenido en materia de seguridad y eficacia.

Existen, en este sentido, numerosos códigos de conducta reguladores del comercio electrónico aprobados en España, si bien en las materias reglamentadas presentan un contenido realmente heterogéneo. Uno de los ámbitos en el que las divergencias resultan ciertamente notorias es, precisamente, el de la seguridad electrónica. Teniendo en consideración tal carácter, efectuaremos una comparación de los diversos códigos de conducta que coexisten a nivel nacional. En cualquier caso, como a propósito del examen de los mismos veremos, su asunción por parte de un determinado prestador de servicios de la sociedad de la información asegura el cumplimiento integral de la normativa legal imperante en materia de comercio electrónico más un plus adicional especialmente tuitivo para el potencial consumidor y/o usuario, extremo especialmente apreciable en el ámbito de la seguridad.

2. ALCANCE DE LA SEGURIDAD ELECTRÓNICA EN FUNCIÓN DE LA ETAPA CONTRACTUAL

Como hemos adelantado, examinaremos las medidas de seguridad implantadas, en las diferentes fases de la relación contractual electrónica, teniendo en cuenta las particularidades de la concreta actividad a la que la misma se aplican. En este sentido, debe anticiparse que los mecanismos técnicos implantados, a tal efecto, serán diversos para cada uno de los supuestos como también el tratamiento jurídico de cuanto estudiaremos. En cualquier caso, debemos considerar que se tratan de cuestiones estrechamente interrelacionadas. En efecto, el Derecho, generalmente, va por detrás de la sociedad y, en el caso que nos ocupa, el legislador regula teniendo en cuenta los medios técnicos ya surgidos, sin perjuicio de que, en alguna ocasión, emplea cláusulas abiertas con la única finalidad de que la normativa no quede obsoleta en un corto espacio de tiempo. Sin embargo, como podemos entender, las modificaciones legislativas deberán, en este campo, acometerse con extremada celeridad pues las nuevas tecnologías, como es

sabido, evolucionan de forma extraordinariamente vertiginosa (Montesinos García, 2007). Hemos de advertir que las nuevas tecnologías no son, en modo alguno, una amenaza para la sociedad sino que representan una ayuda para los operadores jurídicos para, sin duda, actuar con mayor eficiencia (Melos Vázquez, 2002).

Ha de precisarse que, en las diversas fases, deberán cumplirse, en todo caso, ciertos presupuestos que garanticen la seguridad integral de las comunicaciones electrónicas. La conclusión de un contrato en el mercado virtual precisa del envío y recepción, entre las partes contratantes, de manera recíproca, de diferentes comunicaciones electrónicas. La garantía de la seguridad en el intercambio de dichas comunicaciones electrónicas depende del efectivo cumplimiento de cuatro garantías (Font, 2000; Roselló Moreno, 2001; Alonso Ureba y Viera González, 2003; Rodríguez Adrados, 2004; Lafuente Sánchez, 2005; Ferrer Gomila, 2006; Martínez González, 2007; Vázquez Ruano, 2007). En primer lugar, la autenticidad del individuo –con cuya expresión nos referimos a ambas partes: usuario y empresa- que emite la comunicación que pretende garantizar que ese sujeto y no otro es el que ha emitido el mensaje en cuestión. La integridad de la comunicación, en segundo lugar, asegura que la información remitida realmente llega a su destino previsto y que, durante la transmisión, no haya sido alterada accidental o deliberadamente. En tercer término, la confidencialidad de las comunicaciones electrónicas debe entenderse en el sentido de la privacidad del contenido del mensaje que se transmite. Y, por último, el no repudio asegura al remitente que su información ha llegado a su destino y al receptor la identidad del remitente, de manera que cada parte no pueda negar posteriormente su participación en la comunicación entre ambas partes. En definitiva, el comercio electrónico, en general, y el intercambio de comunicaciones, en particular, precisan del establecimiento de instrumentos que acrediten la autenticación y la seguridad de los datos transmitidos (Vázquez Ruano, 2007).

Uno de los instrumentos que existen para garantizar el cumplimiento de las garantías anteriormente enunciadas es la denominada criptografía que podemos definir como un conjunto de técnicas que permiten cifrar y descifrar la información (Moreno Navarrete, 1999; Roselló Moreno, 2001; Ramió Aguirre, 2006). Los mecanismos empleados para cifrar y descifrar son las denominadas "claves" que se asimilan a números de gran longitud con la finalidad de que, precisamente, sean seguras y que siguen un algoritmo matemático. Existen dos grandes técnicas para encriptar y desencriptar: la de cifrado simétrico y la de cifrado asimétrico. La primera es más sencilla que la otra, pues la misma clave es compartida por el emisor y el receptor con los riesgos que, naturalmente, tal circunstancia conlleva. En la técnica de cifrado asimétrico se utilizan dos claves –pública y privada- que, evidentemente, son diversas y que están asociadas, de forma que lo que se cifra con una sólo puede ser descifrado con su pareja y viceversa.

2.1. Relación precontractual

Antes de iniciar cualquier operación para la contratación electrónica de un determinado bien o servicio debemos asegurarnos de la fiabilidad que el vendedor pretende inspirar. Éste puede aseverar, por diversos medios, el cumplimiento de la legalidad imperante en materia sobre todo de privacidad y seguridad mediante la declaración de políticas unilaterales en tal sentido. Sin embargo, no debe darse total y absoluta credibilidad a tales manifestaciones pues la veracidad de la autodeclaración de ciertas prácticas, con independencia de su contenido, dependen de elementos únicamente vinculados a su emisor. La ausencia de sanciones, en caso de violentar los compromisos establecidos con carácter previo, o la falta de control por un tercero independiente son factores que caracterizan a este tipo de políticas empresariales.

En cualquier caso, existen ciertos indicadores de la seguridad de un determinado sitio *Web* que no deberían pasar desapercibidos por un potencial consumidor o usuario. Así, entre otros, procede destacar algunos elementos visuales en materia de seguridad (que acontece

cuando el servidor *Web* utiliza el protocolo de seguridad SSL –capa de conexión segura- que estudiaremos con detenimiento en el apartado siguiente):

1. Que en la dirección de la página *Web* conste una "s" –representativa de la palabra *security*-, tras "*http*", de forma que la dirección comenzaría por "*https*".
2. En la parte inferior derecha de la pantalla puede vislumbrarse, según el navegador utilizado, una imagen de un candado cerrado o de una llave completa que, al pulsarlo, el consumidor o usuario podrá comprobar que el servidor *Web* del vendedor posee un certificado digital de identidad reconocido por un prestador de servicios de certificación. Tal documento, en efecto, incluye datos identificativos de una persona o entidad siendo, en todo caso, la autoridad certificadora –como, por ejemplo, *Verisign*, *Taote*, *Cybertrust*, y *Nortel*-, responsable de los datos que figuren en el certificado. Como podemos observar, una de las funciones más significativas que estas entidades cumplen es la de dar fe de la relación que existe entre los datos que constan en el certificado y la persona o entidad que lo ha solicitado (Martínez Ballesté, 2006).
3. Con carácter previo a la entrada en el portal o página que pretendamos visualizar puede aparecer un mensaje emergente del navegador que nos pregunta si deseamos acceder a un servidor seguro.
4. La adhesión a uno o varios sellos de calidad en materia de comercio electrónico mediante la muestra del logotipo acreditativo y, en virtud de la pulsación en el icono, su acceso electrónico.

Debemos ser conscientes de que la seguridad, en la fase contractual que venimos examinando, también se proyecta en la garantía de la protección de los datos personales de los sujetos que forman parte del acuerdo transaccional electrónico. En efecto, deberán implantarse medidas de seguridad que aseguren un adecuado nivel de amparo, según la tipología, de los datos personales facilitados por los consumidores o usuarios.

2.2. Perfección del contrato: pago de la transacción

Cuando un contrato electrónico se perfecciona las partes contratantes deben cumplir las obligaciones asumidas. Así, por un lado, el vendedor debe entregar el producto o realizar el servicio contratado mientras que, por otro lado, el comprador ha de abonar el precio (Castaingts Teillery, 2002; González, Ferreyros y Carrascosa, 2004; Vicente Blanco, 2007). En el caso del comercio electrónico directo –en el que toda la operativa de la contratación se efectúa por medios telemáticos- el cumplimiento de las obligaciones enunciadas tendrá lugar íntegramente de forma electrónica, mientras que en el indirecto –que se refiere a aquel en el que, al menos, una o varias de las operaciones vinculadas a la contratación electrónica se efectúan a través de medios tradicionales y, por tanto, fuera del mundo virtual- la realización de ciertos deberes podrá tener, y de hecho así será, lugar en el mundo físico. Podemos afirmar que el desarrollo y posterior consolidación del comercio electrónico directo tendrá lugar cuando el pago de la transacción efectuada pueda realizarse de una forma verdaderamente segura (Martínez Nadal, 2006).

El momento del abono de la operación electrónica, para un importante número de consumidores y/o usuarios, puede resultar el más incierto (Ramos Suárez, 2001; Gourion y Ruano-Philippeau, 2003; Vega Vega, 2005). Los usuarios, obviamente, desean utilizar sistemas de pago que les inspiren la misma confianza que los sistemas que utilizan en el comercio tradicional (Payeras Capellá, 2005). La causa de toda la problemática que enunciamos es, sin duda, la falta de seguridad percibida a tal efecto. Es por ello que, como en el siguiente apartado veremos, los códigos de conducta reivindican la implementación de las más avanzadas técnicas existentes al respecto.

Por lo que se refiere a las diversas modalidades más empleadas en materia de contratación electrónica, incluidas dentro del dinero electrónico, destacan la tarjeta de crédito y débito, la denominada tarjeta monedero o de prepago, el pago a través de teléfono móvil,

amén de otras cuales son las plataformas de pago a través de terceros independientes como el servicio de Epagado. A todas ellas nos referiremos en el presente trabajo.

Una de las preocupaciones más significativas del potencial consumidor o usuario a la hora de adquirir, de forma electrónica, un determinado bien o servicio es facilitar los datos vinculados al medio de pago –generalmente tarjeta de débito o crédito- como su nombre completo, fecha de caducidad, número de tarjeta, entidad financiera y otros adicionales. Existen ciertos medios de pago, que buscan mitigar tal desconfianza, como la transferencia bancaria o el pago contrarrembolso que parecen ser los más seguros.

Sin embargo, el medio más empleado en la actualidad para abonar las transacciones electrónicas es la tarjeta de débito o crédito. Antes de ocuparnos de las medidas técnicas ideadas para garantizar elevados niveles de seguridad en materia de contratación electrónica procede referirse, de manera breve, a la problemática que se plantea cuando se realiza un uso ilegítimo de las tarjetas bancarias.

En efecto, como la práctica pone de relieve, la contratación electrónica plantea nuevas formas de utilización ilegítima de la tarjeta bancaria por terceros. En tal modalidad de contratación, la tarjeta bancaria no se presenta, de manera directa, al establecimiento adherido por quien, en ese momento, disfruta de su tenencia sino que este último transmite los datos solicitados entre los que, como regla general, estarán el número de la tarjeta bancaria y otros datos identificativos establecidos para la contratación del bien o servicio. Es perfectamente posible, pues la experiencia así lo confirma en reiteradas ocasiones, que un tercero se apropie, de manera ilícita, de los datos de la tarjeta y de los de su titular y efectúe pagos, por medio de aquélla, en nombre de este último (Mariño López, 2006).

Lo realmente importante para el comercio electrónico es, en cualquier caso, la posible responsabilidad de la entidad emisora de la tarjeta por el uso fraudulento que se pueda realizar por parte de un usuario diverso del titular de la misma (Martínez González, 2007).

En este sentido, el art. 46.1 Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista –LOCM- introduce dos normas en la regulación de las cuestiones que se planteen a propósito del recurso en Internet de las tarjetas bancarias.

En primer lugar, cuando el importe de la compra hubiera sido cargado fraudulenta o indebidamente, utilizando el número de una tarjeta de pago, el 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 posible.

El precepto que examinamos, como dispone Sánchez-Calero Guilarte (2004), no es, en rigor, una norma de protección del consumidor sino una previsión oportuna que orienta su tutela hacia la figura del titular de la tarjeta. El art. 46.1 LOCM parte, asimismo, de la eventual invocación, en una operación, del número de una tarjeta por quien no es su titular, posibilidad que, dicho sea de paso, viene favorecida por la no aprobación física o electrónica de la tarjeta citada.

Es indiferente que la tarjeta sea de crédito o de débito e, igualmente, lo es la entidad que la haya emitido (Marín López, 1996; Fernández-Albor, 2001; Domínguez Luelmo, 2007). La entidad bancaria tiene la obligación de atender, de forma inmediata, la petición de anulación así como de efectuar los correspondientes abono y reabono en las cuentas del proveedor y titular a la mayor brevedad. A pesar de ello, continúan existiendo cláusulas en los contratos bancarios, como ha denunciado ADICAE (2006), que presumen la falta de diligencia en la custodia de la tarjeta.

La expresión “a la mayor brevedad posible” constituye un concepto jurídico excesivamente laxo que podría ser objeto de interpretación según el supuesto concreto y, por tanto, generar una cierta inseguridad jurídica (Guimaraes, 2007). En este sentido, la doctrina no es unánime en la interpretación de la expresión “a la mayor brevedad”. Según una corriente doctrinal, que se ha pronunciado sobre el particular (Bercovitz Rodríguez-Cano, 1997; Peña López, 2005), el tiempo de reabono no debería exceder el plazo de 30 días señalado para devolver el dinero de la venta en el art. 43.2 LOCM. De acuerdo con tal interpretación, si el vendedor

excediese dicho plazo debería indemnizar al titular de la tarjeta los daños y perjuicios que le cause. Si el vendedor se negase a realizar la anulación del cargo o reabono podría, además de cometer un ilícito civil, estar incurriendo en un delito de apropiación indebida.

Según otros autores (Reverte Navarro, 1999), la interpretación que –del término "a la mayor brevedad"- efectúa la anterior postura doctrinal enunciada es errónea pues otorga al vendedor un plazo de tiempo excesivo -30 días-. Entienden que debe aplicarse el plazo de siete días hábiles previstos para el ejercicio del derecho de desistimiento del art. 6.1 de la Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia.

Naturalmente, cabe apuntar que la utilización de la tarjeta robada, hurtada o extraviada para adquirir productos o contratar servicios, cargándolos a la cuenta del titular de la misma constituye un delito de estafa siempre, claro es, que se den todos los elementos integrantes de esta infracción (Orts Berenguer y Roig Torres, 2006; Ruiz, 2006).

En segundo lugar, si la compra hubiera sido efectivamente realizada por el titular de la tarjeta y la exigencia de la devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución, reconocido en el art. 44 LOCM y, por tanto, hubiese exigido indebidamente la anulación del cargo, aquél quedará obligado frente al vendedor al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación (Marín López, 1996; Bercovitz Rodríguez-Cano, 1997; Clemente Meoro, 2000; Vega Vega, 2005; Pendón Meléndez, 2008).

La jurisprudencia se ha pronunciado sobre la cuestión que examinamos en numerosas resoluciones en las que destacan, en unos casos, la atribución de la responsabilidad a la entidad bancaria –entre otras, SAP de Cáceres de 28 de enero de 2004, SJPI de Donostia de 13 de octubre de 2004 y SAP de Madrid de 3 de octubre de 2005- y, en otras, al empresario, proveedor, comerciante o establecimiento comercial –entre otras, SAP de Barcelona de 27 de octubre de 2004, SAP de Barcelona de 22 de diciembre de 2004, SAP de Asturias de 14 de marzo de 2005, SAP de Málaga de 19 de diciembre de 2005 y SAP de La Coruña de 25 de abril de 2006-.

Procede, en línea con las consideraciones que acabamos de examinar, hacer alusión al comercio electrónico seguro, protocolo global de Comercio Electrónico Seguro, instaurado para dotar de una mayor seguridad a las tarjetas Visa y MasterCard cuando se opere, haciendo uso de las mismas, en Internet.

En efecto, cuando el titular de la tarjeta efectúe compras a través de Internet dispondrá de un PIN – *Personal Identification Number*-, o clave personal que, obviamente, sólo deberá ser conocido por él –siendo naturalmente lo más aconsejable para evitar posibles compras y correspondientes cargos no deseados en la cuenta corriente bancaria asociada a la tarjeta de crédito o débito-, que no constará, por evidentes motivos de seguridad, en la tarjeta, a diferencia de lo que sí acontece con el nombre completo del titular, entidad bancaria, número de la tarjeta, fecha de caducidad y código de validación.

Las ventajas del sistema que examinamos son, entre otras, las dos siguientes: 1) identificación plena del usuario de la tarjeta, evitando el uso fraudulento de la misma. Nadie podrá hacer una compra en Internet si desconoce la clave personal, de uso exclusivo, a la que hemos hecho referencia. De esta forma, se evita, por parte del cliente, el repudio de la compra efectuada pues el PIN únicamente es conocido por él que, dicho sea de paso, al teclearlo pone de manifiesto que la compra inequívocamente es realizada por sí mismo o, en su caso, persona autorizada por aquél; 2) identificación de los comercios adheridos al sistema a través de las marcas establecidas al respecto.

Para asegurar un elevado nivel de seguridad, en este sentido, se han implantado diversos protocolos de seguridad que pretenden garantizar las cuatro garantías, que antes examinamos, de toda comunicación electrónica, a saber: autenticidad, integridad, confidencialidad y no repudio. Entre los protocolos más extendidos destaca el SSL –*Secure Socket Layer*-, así como los desarrollados pero no implantados como

SET –*Secure Electronic Transaction*- y STT –*Secure Transaction Technology*-.

Posteriormente aludiremos, someramente, a otros medios de pago como las plataformas de pago a través de terceros independientes que, en algunos supuestos, haciendo uso del protocolo SSL, pretenden, asimismo, incrementar la confianza en los instrumentos de pago –*Paypal*, *Cybercash* y *Epagado*-. Otros, por el contrario, no operan con tal protocolo, como es el caso del pago por móvil y los monederos electrónicos.

El protocolo SSL de *Netscape Comunications Corporation* autentica los servidores *Web*, encripta las comunicaciones y preserva la integridad de los mensajes creando una conexión recíproca entre las partes –cliente y servidor-. El protocolo SSL cifra los datos que entran y salen del servidor –*https*-, hacia o desde el cliente, por lo que la información enviada llegará de manera privada, confidencial e íntegra al servidor del lado del cliente. Uno de los problemas más significativos del sistema que examinamos –SSL-, es que en el momento del formulario de pago se facilitan demasiados datos, por parte del cliente, que únicamente son confidenciales en el tránsito del cliente al servidor. El SSL presenta una serie de deficiencias de seguridad en cuanto a las condiciones que debe reunir un sistema de pago electrónico, a saber:

1. Confidencialidad: la comunicación debe estar restringida sólo a las partes implicadas. SSL garantiza la confidencialidad extremo a extremo pero una vez finalizada la conexión, el vendedor posee todos los datos del comprador, así como su número de tarjeta de crédito. El vendedor podría almacenar esos datos y el cliente estaría expuesto a cualquier tipo de fraude por parte de toda persona que tuviera acceso a dicha información.
2. Integridad: las partes han de tener la garantía de que no se realice modificación alguna en el proceso de comunicación y almacenaje de los datos. SSL no garantiza la integridad de la información una vez finalizada la conexión, sólo durante la transmisión, por lo que el vendedor podría modificar esos datos, por ejemplo, cobrando de más al cliente.
3. Autentificación: las partes deben tener la certeza de que son quien dicen ser. Un cliente no está obligado a autentificarse, una persona con acceso a números de tarjeta de crédito robados puede hacer compras por Internet. Este es el tipo de fraude más común y que causa mayores perdidas a las compañías de crédito y a las tiendas virtuales. Por el lado del vendedor si, además del protocolo de seguridad SSL, el servidor *Web* de la tienda dispone de un certificado electrónico, con éste el cliente verifica que el vendedor sea el servidor de comercio electrónico al que quiere dirigirse.
4. No repudio: las partes no pueden negar haber intervenido una vez realizada la operación. Habida cuenta de la no concurrencia de la autenticación de una de las partes, en concreto de la parte del cliente –el servidor de la tienda *Web* si se autentifica-, no se puede cumplir el requisito del no repudio ya que el cliente puede acogerse a la opción de que no ha realizado la transacción.

Existe una modalidad de protocolo SSL denominado *Extended Validation* –protocolo SSL con Validación Extendida-. El objetivo de este nuevo estándar es combatir el aumento de amenazas en Internet como, por ejemplo, las suplantaciones de identidad –*phishing*-. El nuevo modelo requiere un proceso estricto de autenticación de sitio *Web* y es considerado el "punto de referencia" del sector del comercio electrónico para autenticar la identidad legítima de un sitio *Web*. Asimismo, ofrece a las empresas y a los usuarios en línea un nivel de protección ampliamente reconocido frente a las complejas amenazas en aumento de suplantación de identidad en Internet. Debemos insistir en que el estándar que examinamos incluye una serie de mejoras en la interfaz del sitio *Web* para facilitar al usuario final la identificación de un sitio autenticado.

Los nuevos exploradores de alta seguridad muestran los certificados SSL de Validación Extendida de un modo distinto a los certificados SSL convencionales. En lugar del discreto símbolo de candado que aparece en los certificados SSL tradicionales, los certificados que

comentamos activan la barra de direcciones en exploradores de alta seguridad para mostrar un color verde llamativo. Este cambio es evidente, de inmediato, para el usuario final e incrementa, qué duda cabe, su confianza. Además del sugestivo color verde, la barra de estado de seguridad muestra en un lugar visible el nombre del propietario del sitio *Web* y la autoridad de certificación que ha emitido el certificado. Al igual que con los certificados SSL convencionales, los certificados que estudiamos facilitan la comunicación cifrada segura entre el sitio *Web* y el explorador del usuario. Además, se autentica la identidad original del sitio *Web* de modo que todos los usuarios puedan estar en condiciones de conocer que se han dirigido al sitio *Web* que tenían previsto visitar y no a un sitio falsificado.

En la actualidad, la gran mayoría del *software* que hace uso de Internet, de una forma u otra, cuenta con soporte para SSL, ya que este protocolo se ha convertido en el estándar de protección de información en Internet (Izquierdo Manzanares, 2006).

El Terminal Punto de Venta –TPV- virtual es un programa informático, dirigido a empresas y comercios, con tienda en Internet, que permite el cobro de las ventas de bienes y servicios realizadas en la Red, de forma rápida y segura, cuando el pago de las mismas se realice con tarjeta bancaria. La Pasarela de Pagos o TPV virtual es la solución específica para aquellos establecimientos que desean comercializar y cobrar sus productos a través de Internet. Mediante este sistema, e independientemente de otras formas de pago complementarias que quiera utilizar, los potenciales consumidores y/o usuarios podrán pagar a través de tarjetas bancarias el importe de las compras que efectúen en el sitio *Web* en el momento de realizar el pedido.

El TPV virtual suele hacer uso del protocolo de seguridad SSL y del certificado digital del servidor *Web*. Del primero ya nos hemos ocupado anteriormente, por lo que estimamos oportuno hacer unas breves consideraciones respecto al certificado digital que funciona, junto al protocolo SSL, para evitar que se suplante la identidad de un sitio *Web*. El certificado contiene los datos, avalados por una autoridad certificadora, de la empresa que es dueña del sitio *Web* y que se autentifica con el producto.

El funcionamiento de la Pasarela de Pagos o TPV virtual, por lo demás, es similar al de los TPV's que se encuentran en las tiendas o establecimientos físicos. Cuando el cliente se conecta al sitio *Web* de la empresa y realiza una compra:

1. El sitio *Web* muestra la información del pedido que ha realizado el consumidor y/o usuario, número de artículos, importe, referencia, etc.
2. Si el cliente desea realizar el pago, se conecta a una página segura donde se le solicita el número de su tarjeta bancaria, mes y año de caducidad, tres o cuatro dígitos de seguridad del reverso y, en caso de que esté securizada, además, el PIN asociado a la tarjeta. Los datos de la tarjeta viajan cifrados a la entidad bancaria para que tramite su autorización, es decir, con toda seguridad sin que el empresario tenga acceso a esos datos, de modo que sólo tiene información del pedido (importe, producto, etc.). Sin embargo, la entidad bancaria conoce los datos de la tarjeta pero no del pedido. El TPV virtual incorpora, como hemos anticipado, el protocolo SSL. Además, ese TPV puede funcionar con tarjetas VISA y MasterCard securizadas, es decir, siguiendo las indicaciones del comercio electrónico seguro que obliga a que el usuario teclee un PIN que no consta en la tarjeta. Estos sistemas permiten identificar al comprador que utiliza su tarjeta, como medio de pago, en una tienda virtual. Previamente, el usuario de la tarjeta debe solicitar a su banco el PIN para realizar compras. Con este nuevo modelo, la venta no puede ser rechazada o repudiada siendo, por tanto, una venta garantizada para el comercio.
3. Una vez autorizada la transacción por la entidad emisora de la tarjeta, el TPV virtual le informa tanto al comprador como al empresario del resultado y devuelve el control de la operación a la tienda virtual.

4. En el caso de que la transacción se haya autorizado, el empresario tramitaría la compra y procedería al envío del producto o la prestación del servicio a favor del comprador.

Los datos de la tarjeta son sólo conocidos por la entidad bancaria. El número de tarjeta del cliente es introducido en una página segura y en ningún momento se transmiten al establecimiento. También protege la confidencialidad de la compra porque los datos del pago que se realiza –descripción y contenido- no son requeridos por el TPV virtual, sólo el importe final.

Otro protocolo de seguridad, todavía no implantado, entre otras razones, por su extrema complejidad, es SET que, dicho sea de paso, es más avanzado que el anteriormente examinado. Fue desarrollado por *GTE*, *IBM*, *Microsoft*, *Nestcape Comunicaciones Corp*, *SAIC*, Terisa Sistemas, *Verisign*, Visa Internacional y *MasterCard*. Se basa en el uso de certificados digitales para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción en línea basada en el uso de tarjetas de pago y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su desplazamiento entre los diferentes servidores que participan en el proceso. Con ello, se persigue mantener el carácter estrictamente confidencial de los datos, garantizar la integridad de los mismos y autenticar la legitimidad de las entidades o personas que participan en la transacción, creando, así, un protocolo estándar abierto para la industria que sirva de base a la expansión del comercio electrónico por Internet. En el sistema SET la seguridad en las transacciones se ha cuidado hasta el último detalle. De hecho, utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet.

En cuanto a la actuación de terceros independientes en la operación de pago de la transacción electrónica nos referiremos a *Paypal*, *Epagado* y *Cybercash*. Su labor se reduce a hacer, precisamente, de intermediario en el pago, de forma que los datos de la tarjeta bancaria del comprador no se facilitarán al vendedor. El vendedor recibirá el pago a través del tercero independiente que será quien cargue el abono de la operación al comprador. Obviamente, a cambio de tal actividad, percibirá una comisión.

Paypal y *Epagado* son plataformas de pago de terceros a través de la tarjeta bancaria previamente seleccionada por Internet. Tanto el consumidor y usuario como el propio vendedor necesitan efectuar todo un procedimiento previo de registro y validación. Como antes señalamos, como consecuencia de la operación de compraventa electrónica, hay que pagar una comisión, generalmente a cargo del vendedor, para la tercera parte independiente –*Epagado* y *Paypal*-. El sistema del proceso de pago no se gestiona por el comerciante sino por el servidor de cada uno de los terceros enunciados. Esto implica que los datos bancarios no son, en ningún caso, conocidos por el vendedor que únicamente dispone de los datos completos precisos para el envío y del bien o servicio adquirido.

Vistas las medidas técnicas de seguridad procede, a continuación, referirse al estándar *Payment Card Industry Data Security Standard* (PCI-DSS), que constituye un marco global para la protección de la información asociada a pagos con tarjetas, redactado por las principales empresas de tarjetas bancarias cuales son Visa, MasterCard, American Express, JCB y Discover, en el que se establecen medidas que garantizan la seguridad del tratamiento de este tipo de información, que es de obligado acatamiento, para cualquier organización que recopile, procese y almacene información de tarjetas bancarias, a partir del 1 de enero de 2008.

El incumplimiento del estándar PCI-DSS, exigido tanto a las entidades financieras como a los comercios que acepten pagos con tarjetas y proveedores de servicios que traten información de titulares de tarjetas, se considera una infracción de los procedimientos operativos que puede dar origen a sanciones y penalizaciones.

Cabe determinar que tal modelo, que contiene un conjunto de medidas dirigidas a garantizar la información asociada a pagos con tarjeta bancaria, protege dos grandes modalidades de datos. Por un lado, la información de los titulares –el número de tarjeta, el nombre del titular y fecha de expiración- y, por otro, la

información sensible de autenticación, banda magnética de la tarjeta, PIN y código de validación que se utiliza para transacciones no presenciales. Asimismo, se establecen normas básicas para estas bases de datos bancarias, además de los habituales antivirus, cortafuegos y parches de seguridad, cuales son la necesidad de que los datos deban estar cifrados y los accesos a la máquina controlados y grabados con la finalidad de que quienes la usen estén adecuadamente identificados.

Aunque la medida que estudiamos no sólo afecta al comercio electrónico a través de Internet sino, además, a cualquier compañía que almacene datos bancarios de manera electrónica está especialmente dirigida a aumentar la seguridad del primero.

Procede, finalmente, poner de relieve que el estándar que examinamos otorga las herramientas y medidas necesarias, precisamente, para ayudar en el desarrollo de una cultura internacional de seguridad entre los comerciantes, propiciando, a su vez, el auge del comercio electrónico.

Existen otras dos grandes modalidades de pago. La primera son las tarjetas que llevan incorporado un microchip en el que se almacenan unidades de valor de una moneda determinada, por un importe concreto, que permite ir pagando hasta que se acabe, consolidándose, de este modo, como un medio prepago (Martínez Nadal, 2000; Gómez Cáceres y Corbalán Sánchez de las Matas, 2001; Madrid Parra, 2001). La recarga monetaria puede hacerse de dos maneras. La primera sería a través de tarjeta bancaria y la segunda, mediante efectivo, presencialmente en la propia entidad de crédito.

La segunda modalidad estaría representada por los bonos que garantizan un mayor anonimato del consumidor o usuario que los adquiere pues, además de ser prepago –y, por tanto, adquirirse por un determinado importe-, constituyen una forma de abono que no incorpora al medio, en sí, ningún dato personal del adquirente. En efecto, lo único que incluyen es un código alfanumérico asociado a un determinado valor económico. Su inclusión en los portales previamente habilitados para ello posibilitará que el consumidor efectúe la contratación de productos y/o servicios. Un ejemplo de esta última tipología serían, entre otros, los bonos Ukash.

Cabe referirse, por último, al pago a través de teléfono móvil, también denominados *m-payments* (Mateo Hernández, 2005), cuyo empleo en la actualidad es verdaderamente ínfimo a pesar de que algunos autores han augurado un futuro ciertamente prometedor (Roda, 2005). Se trata de una modalidad de pago necesariamente vinculada a una o varias tarjetas bancarias así como a una previa habilitación del terminal desde el que se acometerá. En la actualidad, existen diversas plataformas empresariales dedicadas a ello cuales son, a título de ejemplo, Mobypay y CaixaMóvil.

3. VIRTUALIDAD DE LA AUTORREGULACIÓN DEL COMERCIO ELECTRÓNICO

Uno de los factores críticos que, como hemos visto, imposibilitan, en gran medida, la consolidación del comercio electrónico reside en las importantes deficiencias de seguridad que sobre el mismo pivotan. Aunque es cierto que los esfuerzos que sobre el particular se han efectuado han sido muy numerosos no han conseguido establecer un nivel de seguridad total. Hemos examinado que las medidas técnicas y legislativas van en la línea de perseguir la implantación de altas cotas de seguridad electrónica sin perjuicio de que, como la experiencia pone de relieve, la rápida obsolescencia de las prácticas realizadas aconsejan una constante y rápida actualización de los agentes responsables.

El legislador nacional no disciplina, de forma expresa, la seguridad electrónica. En otras palabras, no se ha aprobado, por el momento, normativa expresa que regule, de manera integral, las medidas que los prestadores de servicios de la sociedad de la información deben, necesariamente, de poner en práctica para garantizar unos niveles óptimos con los que pueda sentirse relativamente seguro el consumidor y/o usuario que opera en Internet.

Aunque tal apreciación es una realidad debe advertirse el enorme acierto en el que el

legislador español incurre cuando realiza una firme apuesta a favor de la autorregulación del comercio electrónico. Se promueve la elaboración de códigos de conducta del comercio electrónico para, como determina la Exposición de Motivos de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico –LSSI-CE-, adaptar los preceptos de la ley a las características específicas de cada sector. A este respecto, el art. 18.2 párrafo segundo LSSI-CE establece la necesidad de fomentar los códigos de conducta que, entre otros contenidos, abordarán las cuestiones vinculadas con la seguridad electrónica.

4. LOS CÓDIGOS DE CONDUCTA COMO PARADIGMA DE REFERENCIA

En virtud del principio de la autonomía de la voluntad, que es uno de los postulados más vigorosos en materia de Derecho privado, son posibles los denominados códigos de conducta. Como ya hemos adelantado, son instrumentos fomentados por el legislador estatal para, precisamente, lograr que sean los propios agentes que en materia de comercio electrónico interactúan los que regulen (con el respeto absoluto a la normativa inderogable por la voluntad de las partes –leyes imperativas-), tal escenario. Seguidamente analizaremos su concepto, contenido en materia de seguridad y su eficacia. También efectuaremos una comparativa, en materia de seguridad, de los diferentes códigos de conducta.

4.1. Concepto

El hecho de que el legislador español no defina el concepto de código de conducta no es, en absoluto, óbice para que dé ciertas pinceladas sobre el mismo en el ámbito del comercio electrónico. Lo que no parece admisible es que regule ampliamente la figura que examinamos pues, de acuerdo con Medina Malo de Molina (2003), de efectuarse podría incurrirse en una contradicción inadmisible. En efecto, no deben establecerse disposiciones legislativas para aquellos instrumentos que, precisamente, buscan servir de sustituto a dicha normativa y evitar su promulgación en aras de una autorregulación pactada, flexible y dinámica.

Los códigos de conducta representan un instrumento de autorregulación de las empresas en sus relaciones con otras empresas o con los consumidores y usuarios con la voluntad de llevar a cabo su cumplimiento (Maluquer de Motes i Bernet, 2003a).

En nuestra opinión, los códigos de conducta en materia de comercio electrónico pueden definirse como documentos, de carácter voluntario, que incluyen un conjunto de principios, reglas o, en definitiva, buenas prácticas, certificables por una tercera parte independiente, en cuya redacción se han tenido en consideración los intereses de asociaciones de consumidores y usuarios, discapacitados u otros colectivos afectados, que disciplinan materias relativas al procedimiento precontractual, contractual y postcontractual por lo que a la contratación electrónica respecta, sin perjuicio de otras cuestiones como la publicidad interactiva, la protección integral de los menores de edad, la privacidad y la seguridad electrónicas amén de otras conexas, cuya finalidad es la instauración y consolidación de la confianza del potencial consumidor y usuario.

El propósito que se persigue a través de la adopción del código de conducta, como acabamos de enunciar, es la promoción de la confianza en materia de comercio electrónico, tanto frente a los competidores como de los consumidores y/o usuarios. Frente a los competidores porque, entre otros factores, el prestador de servicios conoce y da a conocer sus pautas de actuación en una determinada materia evitando, de esta manera, tener que estar alterando –pero sí actualizando-, por sí mismo, prácticas comerciales en atención, sobre todo, a cómo serán las de sus competidores. Frente a los consumidores y/o usuarios –destinatarios de los servicios- porque de manera anticipada y, en todo caso, pública el empresario podrá dar a conocer las condiciones, especialmente en materia de corrección ética y legal, en las que se prestará el producto o servicio adquirido lo que fomentará la confianza en el comercio electrónico (Medina Malo de Molina, 2003).

Las ventajas de estos códigos son muy numerosas, destacando, entre otras, la mayor implicación de los destinatarios de las normas en su elaboración, lo que aumenta la eficacia de las mismas. Se tiende a considerar las normas como propias, autoimpuestas y como absolutamente necesarias para el buen desarrollo y desenvolvimiento del medio en el que surjan, por lo que el cumplimiento espontáneo aumenta considerablemente con respecto a las normas heterorreguladas –que son aquellas impuestas por el sector público-.

Las normas que se recogen en estos códigos suelen estar mucho más adaptadas al problema concreto que quieren solucionar, ya que la elaboración de los mismos se ha efectuado, precisamente, por las personas que se encuentran en una relación más cercana con la problemática a resolver (Galindo Ayuda, 2002).

La manera en la que un determinado prestador de servicios puede acreditar que está comprometido con las mejores prácticas tanto en materia de seguridad como en otras adicionales, pasa por la exhibición, tanto en el propio sitio *Web* como del restante material publicitario, de un sello o logotipo de confianza (Kuhlmann, 1990; Bock, 2000; Kroeber-Riel y Weinberg, 2003).

4.2. Contenido en materia de seguridad

Aunque existen ciertos códigos de conducta reguladores del comercio electrónico con vocación nacional, entre los que cabe destacar los de la Agencia de la Calidad de Internet, E-confia, Optima Web, Aenor, Agace y E-Web, su articulado en materia de seguridad electrónica no es, en modo alguno, idéntico. En este sentido, es apreciable una enorme divergencia de contenidos en materia de seguridad (que puede observarse en la tabla 1 que figura seguidamente), entre los diferentes códigos de conducta. La heterogeneidad representa, por consiguiente, un carácter predicable de los diversos documentos enunciados.

Si bien es cierto que, por lo que a la seguridad electrónica se refiere, el código de conducta de Agace presenta un elenco de previsiones especialmente interesantes sobre el particular debe advertirse que el código ético actualmente más relevante, en materia de comercio electrónico en general y en ámbito territorial español, es el de la Agencia de la Calidad de Internet. Tal entidad **la componen, además de Red.es -Ministerio de Industria-, los Consejos Audiovisuales de Cataluña, Andalucía, Navarra y Andorra, Autocontrol y la** Asociación Española de Comercio Electrónico y Marketing Relacional –**AECEM**-. Como puede apreciarse, nos encontramos ante una asociación sin ánimo de lucro fundada por 7 entidades, 2 de ellas privadas: AECEM y Autocontrol, representando a la industria publicitaria (anunciantes, agencias y medios); y 5 públicas: Consejos Audiovisuales de Andalucía, Andorra, Cataluña y Navarra y el Ministerio de Industria, Comercio y Turismo a través de la entidad pública empresarial Red.es.

El código ético de comercio electrónico y publicidad interactiva de la Agencia de la Calidad de Internet parece adoptar la estructura de una ley. Así lo atestigua el hecho de que, a diferencia de otros códigos de conducta que se ordenan como principios como el de Agace, cuente con un preámbulo, a modo de Exposición de Motivos, y varios títulos subdivididos en capítulos que, a su vez, se encuentran integrados por artículos. Además, consta de una disposición adicional, una final y un anexo sectorial sobre cláusulas tipo y modelos de protección de datos. Interesa poner de relieve que nos encontramos ante un documento pulcramente redactado, con una sistemática cuidada, que, asimismo, presenta la virtud de aunar en un solo texto la multiplicidad de normas aplicables a cualquier operación de contratación electrónica y publicidad interactiva.

Tras este breve paréntesis conviene, sin más preámbulos, referirnos a la cuestión central del presente apartado que no es otra que el contenido del articulado de los diferentes códigos de conducta en materia de seguridad electrónica.

Especialmente completo, por los contenidos abordados sobre el particular, resulta, como hemos anticipado, el código de conducta AGACE. Tal código, teniendo en consideración

TABLA 1
REGULACIÓN DE LA SEGURIDAD POR LOS DIFERENTES CÓDIGOS DE CONDUCTA VIGENTES EN MATERIA DE COMERCIO ELECTRÓNICO

	Agencia Calidad Internet	AGACE	E-WEB	OPTIMA WEB	AENOR	E-CONFIA
Necesidad de adoptar e implantar un plan integral de seguridad		√				
Establecimiento de una política de gestión y administración adecuada de la infraestructura informática		√				
Sistemas informáticos adecuados al tipo de operaciones y volumen de negocio		√				
Obligación de disponer de una infraestructura informática adecuada que garantice disponibilidad del servicio		√				
Obligación de realizar controles periódicos y pruebas de rendimiento de los sistemas		√				
Obligación de disponer de servicio de asistencia técnica de resolución de contingencias		√				
Establecimiento de una política de administración adecuada de parches y actualizaciones		√				
Creación de una política segura de transmisión de datos	√	√				
Establecimiento de normas de seguridad física que protejan acceso a las instalaciones		√				
Elaboración de procedimientos adecuados de gestión y administración de contraseñas y usuarios		√				
Establecimiento de programas antivirus		√				
Establecimiento de una política adecuada de registros para realizar seguimiento de los accesos		√				
Existencia de copias de seguridad que permita reestablecer sistema ante fallo de importancia		√				
Establecimiento de procedimientos ante contingencias que garanticen respuesta rápida y eficaz	√	√				
Establecimiento de procedimientos de detección y actuación frente a accesos no autorizados		√				
Obligación de realizar una auditoría que verifique la adecuación de las medidas de seguridad adoptadas		√				
Establecimiento de las medidas necesarias que garanticen seguridad y confidencialidad datos financieros	√	√		√	√	√
Obligación de disponer de plataforma que posibilite encriptación de datos	√			√		
Obligación de disponer de medios técnicos y humanos adecuados y actualizados	√	√		√		
Obligación de informar previamente sobre el nivel de protección datos financieros	√	√				√
Obligación de informar sobre el empleo de conexiones seguras -SSL o similares-	√	√	√			
Posibilidad de hacer uso de firma electrónica avanzada		√		√		
Obligación de garantizar la integridad de las operaciones	√	√		√		√
Obligación de garantizar no repudio de las operaciones		√		√		
Posibilidad de recuperación frente a eventuales fallos del sistema		√				
Obligación de que el empresario acredite su identidad mediante certificado digital		√	√		√	

Fuente: Elaboración propia

su articulado en materia de seguridad, se erige en un paradigma de referencia en tal ámbito frente a todos los demás.

El código desarrollado por Aptice, a través de su sección Auditoría y Garantía de Calidad para el Comercio Electrónico –AGACE- es, como decimos, uno de los más completos en cuanto a la seguridad electrónica se refiere. Fue elaborado en 2001 sufriendo la última modificación significativa en 2008. Nos encontramos ante un código al que pueden adherirse proveedores de diferentes sectores o ámbitos del comercio electrónico.

Como pone de manifiesto Galindo Ayuda (2002), el citado código fue redactado guiado por el espíritu de obtener su aceptación consensuada por sus socios. Está acompañado por un sello de garantía y la organización correspondiente, que aplica el primero mediante la infraestructura organizativa desarrollada al efecto: la Agencia AGACE.

El código de conducta que comentamos pretende ser un instrumento para la autorregulación de las empresas y entidades públicas en sus relaciones con los usuarios, los ciudadanos, otras empresas y otras entidades públicas que mantienen transacciones electrónicas con las primeras. En la originaria redacción de su contenido se tuvieron en consideración diferentes fuentes: la normativa y principios jurídicos que, en aquel momento, estaban vigentes en España y la Unión Europea sobre Internet, actividades comerciales y actividades administrativas; las regulaciones de otros códigos de conducta existentes en todo el mundo; las opiniones de expertos en las diferentes materias; las distintas concepciones culturales sobre Internet existentes en sociedades concretas, y las experiencias realizadas al efecto en empresas del sector y organismos públicos.

Aunque la variedad de contenidos del código que comentamos es notable analizaremos, de manera somera, las obligaciones que, para garantizar elevados niveles de seguridad electrónica, se establecen. Tales deberes deberán cumplirse por los prestadores de servicios adheridos al código de conducta que examinamos. La obediencia de tales consideraciones generará elevados niveles de confianza en el consumidor y/o usuario que entable relaciones contractuales con la empresa comprometida con el código de conducta.

Como decimos, el código de conducta Agace incluye en su articulado un conjunto de interesantes previsiones relativas a la seguridad e infraestructura informática del prestador de servicios de la sociedad de la información adherido al sistema de autorregulación que analizamos.

Así, en primer término, se establece la necesidad de que la empresa adherida cumpla con ciertos principios de seguridad básicos tanto en sus sistemas informáticos como de telecomunicaciones. Para ello, deberán necesariamente desarrollarse estrategias de seguridad que garanticen ciertos estándares cuales, entre otros, son: la confidencialidad; la integridad; autenticación; control de accesos; no repudio; y plena disponibilidad de los servicios ofrecidos por el prestador de servicios, siendo esta última previsión la capacidad de recuperación frente a fallos del sistema.

En segundo lugar, la empresa adherida deberá implantar un plan integral de seguridad con la finalidad de cumplir las premisas de seguridad. Para la efectividad de la obligación que examinamos se establece la necesidad de acreditar la aplicación de dos fases claramente diferenciables. La primera, relativa al análisis de riesgos, persigue identificar posibles amenazas y puntos débiles así como su eventual impacto sobre la entidad certificada. La segunda, sobre el desarrollo del plan de seguridad integral, tiene la finalidad de ofrecer soluciones a todos los riesgos y amenazas descritos en la primera fase.

Para la puesta en práctica de la segunda de las fases enunciadas deberán ponerse en marcha ciertas medidas entre las que destacan: la política de gestión y administración de equipos; política de administración de parches y actualizaciones que mantenga los equipos permanentemente actualizados; procedimiento de transmisión segura de datos; normas de seguridad física; procedimiento de gestión y administración de usuarios y contraseñas; política de antivirus; política de gestión y almacenamiento de registros; política de copias de seguridad que permitan restaurar el sistema frente a fallos

importantes del mismo; y procedimiento ante incidencias de seguridad del sistema.

Sin perjuicio de la necesidad de pasar por las dos fases descritas, deberán acreditarse otros extremos adicionales cuales, en esencia, son: la asignación de los recursos, técnicos y humanos, necesarios para la implantación del plan de seguridad; realización de una auditoría que permita garantizar que las medidas de seguridad establecidas garantizan, al menos, los niveles de seguridad básicos; y establecimiento de un procedimiento de actualización y modificación del plan de seguridad.

Además de todas las apreciaciones en las que incurre el sistema de autorregulación que comentamos, cabe destacar que el código deontológico incide en la necesidad de que los sistemas informáticos, propios o subcontratados, de la empresa adherida ofrezcan un servicio adecuado al tipo de operaciones y al volumen de negocio lo cual, a su vez, implica, entre otras obligaciones: la necesidad de implementar una infraestructura informática suficiente que garantice la disponibilidad de los sistemas; la necesidad de efectuar controles periódicos y pruebas de rendimiento; y la contratación de un servicio de asistencia informático para garantizar el buen funcionamiento y la rápida reparación de los sistemas informáticos.

En definitiva, pueden ponerse como modelo de seguridad electrónica las interesantes actuaciones desplegadas en materia de autorregulación del comercio electrónico. Tales previsiones representan un sugerente complemento de la legislación sobre el particular. Además, deben ponerse de manifiesto ciertas ventajas que concurren en los denominados códigos de conducta cuales, entre otras, son la constante y rápida actualización de los contenidos presentes en los mismos. Tal aspecto resulta clave en un ámbito, como la seguridad electrónica, donde la misma resulta decisiva. En efecto, aunque el Derecho debe adaptarse a los cambios tecnológicos acontecidos en diferentes sectores –siendo uno de ellos el relativo al comercio electrónico-, la adecuación de la normativa a la realidad social tiene lugar con cierto retraso sobre todo debido a los largos trámites por los que, en ocasiones, habrá que pasar. Tales *handicaps* no concurren en el ámbito de los sistemas de autorregulación erigiéndose, en este sentido, en un complemento muy efectivo de la legislación.

4.3. Eficacia

Los códigos de conducta son compromisos contractuales, no pudiendo ser, en modo alguno, considerados normas jurídicas sin perjuicio de que, como contratos que son, tienen valor o fuerza de ley entre las partes contratantes que, en nuestro caso, serán, por un lado, la empresa responsable del sistema de autorregulación y, por otro, el prestador de servicios de la sociedad de la información adherido al código de conducta si bien, curiosamente, su eficacia fundamentalmente se despliega frente a los potenciales consumidores y/o usuarios de la empresa adherida.

A juicio de un sector de la doctrina (Maluquer de Motes i Bernet, 2003b), los códigos de conducta, merecen, en la actualidad, la consideración de costumbre y, por tanto, son fuente del Derecho. Según tal postura, aquéllos son un estilo, son usos normativos o legislativos. Si admitiéramos tal afirmación, como es sabido, en atención al art. 1 Código civil, los códigos de conducta serían fuente del Derecho aplicables en defecto de Ley. Consideramos, sin embargo, que hoy día no podemos apreciar, por no concurrir los elementos preceptivos para ello, tal naturaleza pues la fuerza que los códigos de conducta ostentan, en la actualidad, es estrictamente convencional teniendo presente que resulta necesaria la previa aceptación, por parte de la empresa, del código de conducta. Su fuerza obligatoria, reiteramos, es estrictamente convencional. Si se tratase de un uso normativo no sería necesario el expreso sometimiento ni el acuerdo previo para su aplicación final.

En cualquier caso, sean o no fuente del Derecho, el papel y función que los códigos de conducta cumplen es la que corresponde a aquéllas (Clemente Meoro y Cavanillas Múgica, 2003). Representan una forma de hacer que se

crea en el marco de una comunidad de empresas, en una asociación de éstas o en un sector de actividad determinado cual es, por ejemplo, el comercio electrónico.

Los códigos deontológicos no tienen, en ningún caso, la coerción de una norma jurídica. Este punto es probablemente su debilidad sin que la misma pueda interpretarse como su ineficacia. Teniendo en consideración que, en la práctica totalidad de las ocasiones, no puede hablarse de un comportamiento ético al margen de la legalidad, el primer mandato ético al que ineludiblemente deben obedecer los sistemas de autorregulación en materia de comercio electrónico estriba en la necesidad de adecuar las operaciones efectuadas en materia de comercio electrónico a la legalidad vigente.

En la medida en que los códigos de conducta estén revestidos de fuerza coactiva podrán transmitir la garantía, seguridad y confianza que se proponen. Tal extremo cabe siempre y cuando se contemple la posibilidad de sanción en la letra de los códigos. En efecto, todo código de conducta debe contemplar un medio coercitivo en forma de sanción. Lo contrario sería considerarlo como una simple declaración de intenciones y, naturalmente, no tendría eficacia ni fuerza vinculante (Maluquer de Motes i Bernet, 2003b). El catálogo de sanciones que el organismo de control (del sistema de autorregulación en el que el código de conducta se integra) podría imponer es realmente amplio. Así, siguiendo a Maluquer de Motes i Bernet (2003b), la sanción que, según el supuesto, podría aplicarse va desde la simple amonestación, advertencia o publicidad de incumplimiento hasta otras como la suspensión de derechos, la fijación del pago de una multa pecuniaria o la expulsión del sistema de autorregulación en cuestión.

En todo caso, como acertadamente dispone Galindo Ayuda (2002), los instrumentos de carácter sancionador establecidos en el articulado de los códigos de conducta actuarán en colaboración con los mecanismos existentes en el Estado de Derecho para la solución extrajudicial de los conflictos que eventualmente puedan plantearse.

Un supuesto especialmente controvertido, en todo el orden de cuestiones que venimos abordando, vendría determinado por el hecho de qué consecuencias podría tener la exhibición del sello de confianza –acreditativo de la adhesión a un determinado código de conducta en materia de comercio electrónico- en el sitio *Web* y/o en diferentes instrumentos o canales publicitarios de la empresa y el posterior incumplimiento que las obligaciones inherentes a su muestra representa (en nuestro caso en materia de seguridad electrónica). En efecto, en el caso de que el prestador de servicios de la sociedad de la información revelara estar comprometido con las prácticas contenidas respecto a la seguridad electrónica en un determinado código de conducta, habrá de ser consecuente con tal comportamiento ya que tal actitud podría ser determinante para la celebración de ciertos contratos por parte de determinados consumidores y/o usuarios que, todo hay que decirlo, en caso de saber que la empresa en cuestión no estaba adherida a código de conducta alguno y, en consecuencia, no infundir una sensación de confianza podrían no haber celebrado.

En tales casos, como es sabido, la publicidad integra el contenido del contrato. Como determina el art. 61.2 Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para Defensa de los Consumidores y Usuarios y otras Leyes complementarias –TRLGDCU- "las condiciones jurídicas o económicas y garantías ofrecidas serán exigibles por los consumidores y usuarios, aún cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido y deberán tenerse en cuenta en la determinación del principio de conformidad con el contrato". Si referimos tal estipulación al ámbito de los códigos de conducta del comercio electrónico habremos de considerar la plena vigencia de las obligaciones asumidas en materia de seguridad por el prestador de servicios de la sociedad de la información. Pudieron ser la concurrencia de las mismas –mediante la exhibición del respectivo logotipo de confianza- las que, precisamente, despertaron la intencionalidad de contratar en el potencial consumidor

y/o usuario que, de buena fe, inició los trámites contractuales necesarios para adquirir, bajo las condiciones de seguridad establecidas en el código de conducta, la actividad comercial publicitada. En consecuencia, como lo ofrecido no coincide con lo publicitado, existiría incumplimiento contractual por parte del prestador de servicios de la sociedad de la información cuya actitud defraudaría las iniciales expectativas del consumidor y/o usuario.

Asimismo, debe considerarse la posible deslealtad del comportamiento recientemente descrito. En efecto, la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior –Directiva sobre prácticas comerciales desleales- ha dado un paso adelante en la imbricación de los sistemas de autocontrol en el régimen de represión de la competencia desleal al incluir entre las prácticas comerciales desleales el incumplimiento de los compromisos asumidos por la adhesión a códigos de conducta en determinadas circunstancias (Massaguer Fuentes, 2006).

El art. 6.2.b) de la Directiva sobre prácticas comerciales desleales sólo considera práctica comercial engañosa el incumplimiento de los compromisos –en nuestro caso en materia de seguridad- asumidos por la adhesión a códigos de conducta, en los casos en los que el empresario haga expresa mención de su sometimiento a tal código entre las alegaciones o manifestaciones realizadas en una práctica comercial. La idea que subyace en este precepto es que cuando una empresa declara su adhesión a un código hace nacer expectativas legítimas. De tal manera que si la empresa no cumpliera el compromiso firme recogido en el código, su comportamiento será considerado como una alegación falsa y, por lo tanto, una práctica desleal en virtud de la Directiva marco.

5. CONCLUSIONES

El comercio electrónico representa una actividad comercial con una importante proyección de futuro si bien existen ciertos factores muy vinculados a la seguridad electrónica que impiden su consolidación efectiva. Para hacer frente a tal extremo el legislador nacional persigue fomentar la adhesión, por parte de los prestadores de servicios de la sociedad de la información, a los códigos de conducta reguladores del comercio electrónico en general que, como hemos analizado, disciplinan aquellos aspectos particularmente relevantes en tal escenario cual es la seguridad.

La adhesión voluntaria a un determinado código de conducta en materia de comercio electrónico garantiza dos cuestiones. Por un lado, que, por parte de las entidades comprometidas con su contenido, se cumple la legalidad imperante sobre la materia más un plus adicional especialmente favorable para el potencial consumidor y/o usuario –que hemos examinado detenidamente para el caso de la seguridad electrónica- y, por otro, que la empresa signataria sería, por parte de la sociedad en general, merecedora de la estimación más positiva en cuanto a operaciones vinculadas, directa o indirectamente, con el comercio electrónico y, asimismo, representativa de aplicar las mejores prácticas empresariales sobre el particular en las que ocupa una especial relevancia la seguridad (Schulz, 1995).

El rol que, en la práctica, tales figuras desempeñan (cuya adhesión se muestra mediante la exhibición del correspondiente icono de confianza) es muy relevante. En efecto, la presencia de los sellos de calidad o confianza en un determinado sitio *Web*, así como la consulta electrónica del contenido de código de conducta cuyo cumplimiento acredita, muestran que el prestador de servicios de la sociedad de la información es, dicho coloquialmente, "de fiar" y que en materia de seguridad electrónica aplicará las técnicas más avanzadas sobre el particular. Como es natural, es, a todos los efectos, muy significativa la imagen que una determinada empresa proyecta ante la opinión pública. El recurso a los instrumentos de confianza que hemos examinado puede resultar muy útil tanto por parte de empresas consolidadas en el mundo físico o tradicional como, con mayor razón, por sociedades emergentes.

6. REFERENCIAS BIBLIOGRÁFICAS

ADICAE (2006) "Los sistemas de pago electrónico: ¿fiables y seguros?", *Impositores, usuarios de bancos, cajas y seguros*, núm. 72.

Alonso Ureba, A. y Viera González, A. J. (2003) "Formación y perfección de los contratos a distancia celebrados por Internet". En Mateu de Ros, R. y López-Monis Gallego, M. (Coords.), *Derecho de Internet: la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico* Thomson Aranzadi, Navarra, pp. 271-385.

Alonso, R. (2001) *Confianza y seguridad en comercio electrónico*, Instituto de Auditores-Censores Jurados de Cuentas y Agrupación Territorial del País Vasco, Bilbao.

Arranz, L. y González Espasas, F. J. (2002) "E-Banking. Medios de pago y servicios financieros". En *Internet. Claves legales para la empresa*, Thomson Civitas, Madrid, pp. 691-741.

Barral Viñals, I. (2003) "La seguridad en Internet: la firma electrónica". En Barral Viñals, I. (Coord.), *La regulación del comercio electrónico*, Dykinson, Madrid, pp. 83-109.

Barreiros Fernández, J. (2002) *El papel del notariado en el uso de la firma digital*, Consejo General del Notariado, Madrid.

Bercovitz Rodríguez-Cano, R. (1997) *Comentarios a las Leyes de Ordenación del Comercio Minorista*, Tecnos, Madrid.

Bock, A. (2000) *Gütezeichen als Qualitätsaussage im digitalen Informationsmarkt*, Toeche-Mittler, Darmstadt.

Boix Palop, A. (2006) "Del equilibrio entre intereses individuales y colectivos. Derecho y garantía pública de la ajustada conciliación de los mismos". En Boix Palop, A. y López García, G. (Eds.), *La autoría en la era digital: industria cultural y medios de comunicación*, Tirant lo Blanch, Valencia, pp. 89-115.

Bolás Alfonso, J. (2000) *Firma electrónica, comercio electrónico y fe pública notarial*, Consejo General del Notariado, Madrid.

Castaingts Teillery, J. (2002) *Simbolismos del dinero. Antropología y economía: una encrucijada*, Anthropos, Barcelona.

Clemente Meoro, M. (2000) "Algunas consideraciones sobre la contratación electrónica", *Revista de Derecho Patrimonial*, núm. 4, pp. 59-86.

Clemente Meoro, M. y Cavanillas Múgica, S. (2003) *Responsabilidad civil y contratos en Internet. Su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Comares, Granada.

De Pablo Redondo, R. (2006) *Internet y la nueva economía en las empresas. Estudio del caso Amadeus*, Instituto de Estudios Económicos, Madrid.

Delgado Bustos, R. (2002) "El comercio electrónico a través del análisis de Webs nacionales". En Méndiz Noguero, A. y Victoria Mas, J. A. (Coords.), *Publicidad, comunicación y Marketing en Internet. Reiniciar el sistema: Actas de las III Jornadas de Publicidad Interactiva*, Área de Cultura y Ecuación de la Diputación Provincial de Málaga, Málaga, pp. 225-235.

Domínguez Luelmo, A. (2007) "Contratación electrónica con consumidores". En Mata y Martín, R. M. (Dir.) y Javato Martín, A. M. (Coord.), *Los medios electrónicos de pago: Problemas Jurídicos*, Comares, Granada, pp. 67-166.

Feliu Rey, M. I. (2002) *La protección del consumidor en Internet. Informe emitido a petición del Consejo de Consumidores y Usuarios*, Consejo de Consumidores y Usuarios, Madrid.

Fernández Gómez, E. I. (2002) "La seguridad en los pagos: la clave para el despegue del B2C", *Harvard Deusto Finanzas y Contabilidad*, núm. 47, pp. 28-43.

Fernández Rodríguez, J. J. (2006) "La aprehensión jurídica de la democracia y el gobierno electrónicos". En Cotino Hueso, L. (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares, Granada, pp. 135-148.

Fernández-Albor Baltar, A. (2001) "Régimen jurídico de la contratación en Internet". En Gómez Segade, J. A. (Dir.), Fernández-Albor Baltar, A. y Tato Plaza, A. (Coords.), *Comercio electrónico en Internet*, Marcial Pons, Madrid-Barcelona, pp. 269-305.

Ferrer Gomila, J. L. (2006) "Seguridad". En Peguera Poch, M. (Coord.), *Firma electrónica y medios de pago en Internet*, Universidad Oberta de Cataluña, Barcelona.

Font, A. (2000) *Seguridad y certificación en el comercio electrónico*, Fundación Retevisión, Madrid.

Galindo Ayuda, F. (2002) "Códigos de conducta para la regulación del comercio y el gobierno electrónicos", *La Ley*, núm. 2, pp. 1873-1882.

García Más, F. J. (1998) "La contratación electrónica: la firma y el documento electrónicos", *Boletín de Información del Colegio Notarial de Granada*, núm. 210.

García Más, F. J. (1999) "La contratación electrónica: la firma y el documento electrónicos", *Revista Crítica de Derecho Inmobiliario*, núm. 652, pp. 765-790.

García Más, F. J. (2000) "El comercio electrónico: contratación y firma electrónicas", *Academia Sevillana del Notariado*, Tomo 13, pp. 183-236.

García Más, F. J. (2004) *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, 2ª edición, Lex Nova, Valladolid.

Gómez Cáceres, D. y Corbalán Sánchez de las Matas, L. (2001) *Mercados electrónicos. Nuevos sistemas de pago*, Esic, Madrid.

González Aguilar, A. Ferreyros Soto, C. y Carrascosa López, C. (2004) *Los contratos en la sociedad de la información. Formularios de contratos informáticos e Internet*, Comares, Granada.

González, E. (1999) "Internet el medio de las mil caras (Breves reflexiones acerca de las normas sobre publicidad aplicables en Internet)", *Revista Autocontrol de la Publicidad*, núm. 33.

Gourion, P. A. y Ruano-Philippeau, M. (2003) *Le droit de Internet dans l´entreprise*, LGDJ, París.

Guimaraes, M. R. (2007) "El pago mediante tarjetas de crédito en el comercio electrónico. Algunos problemas relativos a su naturaleza jurídica, marco contractual y régimen aplicable, desde una perspectiva comparada en los derechos portugués, español y comunitario". En Mata y Martín, R. M. (Dir.) y Javato Martín, A. M. (Coord.), *Los medios electrónicos de pago: Problemas Jurídicos*, Comares, Granada, pp. 167-217.

Izquierdo Manzanares, A. (2006) "Metodología para la validación y evaluación remota de implementaciones de protocolos de seguridad. Aplicación a la arquitectura IPSEC", Tesis doctoral, Universidad Carlos III de Madrid.

Joines, J. L. Scherer, C. W. y Scheufele, D. A. (2003) "Exploring Motivations for Consumer Web Use and their Implications for E-Commerce", *Journal of Consumer Marketing*, Vol. 20, núm. 2, pp. 90-108.

Kalyanam, K. (2002) "The E-Marketing Mix: A Contribution of the E-Tailing Wars", *Journal of the Academy of Marketing Science*, Vol. 30, núm. 4, pp. 487-499.

Korgaonkar, P. K. y Wolin, L. D. (1999) "A Multivariate Analysis of Web Usage", *Journal of Advertising Research*, Vol. 39, núm. 2, pp. 53-68.

Kroeber-Riel, W. y Weinberg, P. (2003) *Konsumentenverhalten*, 8ª edición, Vahlen, Munich.

Kuhlmann, E. (1990) *Verbraucherpolitik: Grundzüge ihrer Theorie und Praxis,* Vahlen, Munich.

Lafuente Sánchez, R. (2005) *Los servicios financieros bancarios electrónicos*, Tirant lo Blanch, Valencia.

Madrid Parra, A. (2001) "Seguridad, pago y entrega en el comercio electrónico", *Revista de Derecho Mercantil*, núm. 241, Julio-Septiembre, pp. 1189-1264.

Madrid Parra, A. (2003) "Seguridad en el Comercio Electrónico". En Orduña Moreno, F. J. (Dir.), y Campuzano Laguillo, A. B. y Plaza Penadés, J. (Coords.), *Contratación y Comercio Electrónico*, Tirant lo Blanch, Valencia, pp. 123-193.

Maluquer de Motes i Bernet, C. J. (2003a) "La solución extrajudicial de los conflictos: códigos de conducta y arbitraje electrónico". En Barral Viñals, I. (Coord.), *La regulación del comercio electrónico*, Dykinson, Madrid, pp. 111-130.

Maluquer de Motes i Bernet, C. J. (2003b) "Los códigos de conducta como fuente del Derecho", *Derecho Privado y Constitución*, núm. 17, pp. 361-376.

Marín López, J. J. (1996) *Ordenación del comercio minorista*, Praxis, Barcelona.

Mariño López, A. (2006) *Uso fraudulento de tarjetas de crédito por terceros no autorizados. Daños y responsabilidad civil*, Marcial Pons, Madrid-Barcelona.

Martínez Ballesté, A. (2006) "Sistemas de pago para el comercio electrónico". En Herrera Joancomartí, J. y Rodríguez Ardua, I. (Coords.), *Tecnologías del comercio electrónico*, Universidad Oberta de Cataluña, Barcelona.

Martínez González, M. (2007) "Mecanismos de seguridad en el pago electrónico". En Mata y Martín, R. M. (Dir.) y Javato Martín, A. M. (Coord.), *Los Medios Electrónicos de Pago. Problemas jurídicos*, Comares, Granada, pp. 5-66.

Martínez Nadal, A. (2000) "Medios de pago en el comercio electrónico", *Actualidad Jurídica Aranzadi*, núm. 37, Octubre, pp. 6-11.

Martínez Nadal, A. (2006) "Dinero electrónico. Medios de pago". En Peguera Poch, M. (Coord.), *Firma electrónica y medios de pago en Internet*, Universidad Oberta de Cataluña, Barcelona, pp. 6-103.

Massaguer Fuentes, J. (2006) *El nuevo derecho contra la competencia desleal. La Directiva 2005/29/CE sobre prácticas comerciales desleales*, Thomson Civitas, Madrid.

Mateo Hernández, J. L. (2005) *El dinero electrónico en Internet. Aspectos técnicos y jurídicos*, Comares, Granada.

Medina Malo de Molina, E. (2003) "Comunicaciones comerciales por vía electrónica: códigos de conducta, resolución judicial y extrajudicial de conflictos". En Mateu de Ros, R. y López-Monis Gallego, M. (Coords.), *Derecho de Internet: la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Thomson Aranzadi, Navarra, pp. 519-554.

Melián Alzola, L. y Padrón Robaina, V. (2005) "El valor en los mercados de consumo B2C". En Gutiérrez Arranz, A. M. y Sánchez-Franco, M. J. (Coords.), *Marketing en Internet. Estrategia y empresa*, Pirámide, Madrid, pp. 59-92.

Melos Vázquez, L. (2002) "El Derecho Procesal y las nuevas tecnologías con especial referencia a las comunicaciones procesales vía e-mail". En *XVII Jornadas iberoamericanas y XI uruguayas de Derecho Procesal*, Fundación de Cultura Universitaria, Montevideo.

Montesinos García, A. (2007) *Arbitraje y Nuevas Tecnologías*, Thomson Civitas, Madrid.

Moreno Navarrete, M. A. (1999) *Contratos Electrónicos*, Marcial Pons, Madrid.

Orts Berenguer, E. y Roig Torres, M. (2006) "Delitos contra la intimidad, utilización fraudulenta de trajetas de cédito y falsedad en documento electrónico: análisis de casos". En Sanjuán y Muñoz, E. (Dir.), *Incorporación de las Nuevas Tecnologías en el comercio: aspectos legales*, Consejo del Poder Judicial, Madrid, pp. 87-128.

Park, J. Lee, D. y Ahn, J. (2004) "Risk-Focused e-Commerce Adoption Model: A Cross-Country Study", *Journal of Global Information Tecnology Management*, Vol. 7, núm. 2, pp. 6-30.

Payeras Capellá, M. M. (2005) "Protocolos de Comercio Electrónico: Pago Anónimo e Intercambio Equitativo", Tesis doctoral, Universidad de las Islas Baleares.

Pendón Meléndez, M. A. (2008) "Reflexiones críticas acerca del régimen legal de las operaciones a distancia (en los contratos celebrados con consumidores y en ventas entre empresarios) tras la entrada en vigor del Real Decreto Legislativo 1/2007, de 16 de noviembre", *Derecho de los Negocios*, núm. 209, pp. 5-34.

Peña López, F. (2005) "La adquisición de bienes y productos por el consumidor". En Busto Lago, J. M. (Coord.), *Reclamaciones de consumo. Derecho de consumo desde la perspectiva del consumidor*, Thomson Aranzadi, Navarra, pp. 341-462.

Plaza Penadés, J. (2003) "Contratación electrónica y pago electrónico (en el derecho nacional e internacional)". En Orduña Moreno, F. J. (Dir.), y Campuzano Laguillo, A. B. y Plaza Penadés, J. (Coords.), *Contratación y Comercio Electrónico*, Tirant lo Blanch, Valencia, pp. 403-475.

Ramió Aguirre, J. (2006) "La seguridad informática y sus amenazas". En Soler Matutes, P. (Dir.), Piattini Velthuis, M. e Ilustre Colegio de Ingeniería en Informática de Cataluña (Coords.), *Manual de Gestión y Contratación Informática*, Thomson Aranzadi, Navarra, pp. 151-164.

Ramos Suárez, F. (2001) "La seguridad jurídica en el comercio electrónico", *Revista de la Contratación Electrónica*, núm. 19, pp. 109-136.

Reverte Navarro, A. (1999) "Artículo 46. Pago mediante tarjeta de crédito". En Alonso Espinosa, F. J. (Coord.), *Régimen jurídico general del comercio minorista: Comentarios a la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista, y a la Ley Orgánica 2/1996, de 15 de enero, complementaria de la*

de ordenación del comercio minorista, McGraw Hill, Madrid, pp. 586-587.

Ribagorda Garnacho, A. (2008) "La dimensión técnica de la protección de datos personales". En *Estudios en Homenaje al profesor Gregorio Peces-Barba: entre la ética, la política y el derecho*, Vol. 1, Dykinson, Madrid, pp. 1127-1142.

Roda, I. (2005) *Los pagos móviles en España: situación actual y perspectivas*, Firma de Información, Madrid.

Rodríguez Adrados, A. (2004) "Firma electrónica y documento electrónico", *Anales de la Real Academia de Jurisprudencia y Legislación*, núm. 34, pp. 381-428.

Roselló Moreno, R. (2001) *El comercio electrónico y la protección del consumidor*, Cedecs, Barcelona.

Rufín Moreno, R. (2008) *Marketing avanzado*, Editorial Sanz y Torres, Madrid.

Ruiz, L. R. (2006) "Uso ilícito y falsificación de tarjetas bancarias", *Revista de los Estudios de Derecho y Ciencia Política de la Universidad Oberta de Cataluña*, núm. 3, pp. 1-12.

Sánchez Bravo, A. A. (2001) "Una política comunitaria de seguridad en Internet", *La Ley*, núm. 7, pp. 1344-1356.

Sánchez-Calero Guilarte J. (2004) "Tarjetas de crédito y tutela del consumidor", *Estudios de Derecho Judicial*, núm. 50, pp. 437-484.

Schulz, W. (1995) "Kampf der Fiktionen: Paragraphen gegen reitende Leichen. Grenzen regulativer und Chancen kontextualer Steuerung von Fernsehinhalten am Beispiel von Gewaltdarstellungen". En Friedrichsen, M. y Vowe, G. (Eds.), *Gewaltdarstellungen in den Medien: Theorien, Fakten und Analysen*, Westdeutscher Verlag, Opladen, pp. 349-367.

Sisodia, R. S. y Wolfe, D. B. (2000) "Information Technology: Its Role in Building, Maintaining and Enhance Relationship". En *Handboock of Relationship Marketing*, Sage Publications.

Vázquez Ruano, T. (2007) "La seguridad electrónica en la fase precontractual. Un apunte desde el derecho comunitario". En Madrid Parra, A. (Dir.), y Guerrero Lebrón, M. J. (Coord.), *Derecho Patrimonial y Tecnología. Revisión de los principios de la contratación electrónica con motivo del Convenio de las Naciones Unidad sobre Contratación Electrónica de 23 de noviembre de 2005 y de las últimas novedades legislativas*, Marcial Pons, Madrid-Barcelona, pp. 251-274.

Vega Vega, J. A. (2005) *Contratos Electrónicos y Protección de los Consumidores*, Reus, Madrid.

Vicente Blanco, D. J. (2007) "Medios electrónicos de pago y jurisdicción competente en supuestos de contratos transfronterizos en Europa (Los criterios de competencia judicial del derecho comunitario europeo y su aplicación a las relaciones contractuales involucradas en los medios electrónicos de pago)". En Mata y Martín, R. M. (Dir.) y Javato Martín, A. M. (Coord.), *Los medios electrónicos de pago: Problemas Jurídicos*, Comares, Granada, pp. 269-318.

Vilches Trasierra, J. A. (2002) *Aproximación a la Sociedad de la Información: Firma, Comercio y Banca Electrónica*, 2ª edición, Centro de Estudios Registrales, Madrid.

Villanueva, J. y Iniesta, F. (2001) "Factores inhibidores en la adopción de Internet como canal de compra", *Economía Industrial*, núm. 340, pp. 93-100.