LA PROTECCIÓN DE LOS CONSUMIDORES EN LAS TRANSACCIONES ELECTRÓNICAS DE PAGO

(Consumer protection in electronic payment transactions)

Mariliana Rico Carrillo
Universidad Católica del Táchira - Venezuela

RESUMEN

El presente artículo tiene por objeto el estudio de la protección de los consumidores en las transacciones electrónicas de pago a la luz de las previsiones de la legislación venezolana. Para determinar los derechos del consumidor en este aspecto se analizan los mecanismos de seguridad, tanto técnicos como jurídicos que deben estar presentes en una transacción de pago. Un mecanismo de pago seguro debe garantizar la confidencialidad y la privacidad de la operación, la indicación del riesgo y la determinación de responsabilidad por usos fraudulentos o no autorizados.

Palabras Clave: Pagos electrónicos, Seguridad, Privacidad, Confidencialidad

ABSTRACT

This document studies consumer protection in electronic payment transactions in Venezuelan legislation. In order to determine the rights of the consumer in this aspect, technical and legal security mechanisms that must be provided in such operations are analysed. A secure payment method must guarantee the confidentiality and privacy of the transaction, the signalling of risks and the determination of liability for fraudulent or non-authorized use.

Key words: Electronic payments. Security. Privacy. Confidentiality.

INTRODUCCIÓN

La seguridad en los sistemas de pago es considerada un elemento decisivo para el desarrollo del comercio electrónico [1], entre las cuestiones más importantes en este ámbito destacan la necesidad de garantizar la seguridad jurídica de la transacción, la privacidad de la operación y la prevención sobre el uso fraudulento de los medios de pago.

En Venezuela, las normas sobre protección de los consumidores en las transacciones de pago se encuentran incluidas en el Capítulo V de la Ley de Protección al Consumidor y Usuario [2], que regula las operaciones del comercio electrónico realizadas entre proveedores de bienes y servicios y consumidores. La mayor preocupación del legislador en este ámbito se centra garantizar la seguridad,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

esta situación se desprende del contenido del artículo 40, al establecer la obligación de proporcionar al consumidor mecanismos fáciles y seguros de pago.

El concepto de seguridad en las transacciones electrónicas es amplio y abarca fundamentalmente dos aspectos: el técnico y el jurídico. La seguridad jurídica implica la definición de los derechos y obligaciones de las partes a efectos de determinar a quién corresponde la responsabilidad en caso de una determinada actuación, también comprende la protección del derecho a la privacidad y la confidencialidad de la operación. La seguridad técnica constituye una herramienta fundamental al auxilio de la seguridad jurídica, la tecnología ofrece diversos mecanismos que facilitan el cumplimiento de las obligaciones de seguridad impuestas a los proveedores, los métodos de cifrado son ejemplo de ello, ya que permiten ocultar la información, proporcionando la confidencialidad y privacidad de la operación, requisitos exigidos por la ley para garantizar la protección de los consumidores y usuarios.

A continuación se realiza un estudio sobre la protección de los consumidores en las transacciones electrónicas de pago, nuestra investigación tiene como propósito la determinación del contenido de la obligación establecida en la ley de suministrar mecanismos fáciles y seguros de pago. La finalidad principal de este trabajo se centra en establecer los requisitos que deben cumplirse para que un sistema de pago pueda calificarse como seguro. Para alcanzar los objetivos propuestos, se analizan los sistemas de seguridad, tanto técnicos como jurídicos que -en nuestra opinión- deben estar presentes en las operaciones de pago para considerar que se han preservado los derechos de los consumidores en este aspecto.

LA PROTECCIÓN DE LOS CONSUMIDORES EN EL COMERCIO ELECTRÓNICO

Marco legal

La Ley de Protección al Consumidor y Usuario de 2004 (en adelante LPCU) introduce un aspecto de especial importancia en la tutela de los derechos de los consumidores, al consagrar en el Capítulo V, la protección específica en el ámbito del comercio electrónico, entendiendo por tal: *"…cualquier forma de negocio, transacciones comerciales o intercambio de información publicitaria con fines comerciales, que sea ejecutada a través del uso de tecnologías de información y comunicación".*

Siguiendo las orientaciones internacionales, la ley venezolana adopta una noción amplia de lo que debe entenderse por comercio electrónico, abarcando cualquier operación comercial que sea ejecutada a través del uso de tecnologías de información y comunicación, concepto que incluye, lógicamente, las transacciones realizadas a través de redes abiertas de comunicación como Internet, donde los consumidores exigen mayor protección.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

La defensa de los consumidores en el ámbito de las transacciones electrónicas tiene por objeto reforzar la protección que normalmente se otorga a estos sujetos en las operaciones tradicionales, ello quiere decir que, además de los derechos específicos consagrados en la LPCU para las transacciones comerciales electrónicas, el consumidor también gozará de los demás derechos que le otorga la ley, que sean aplicables al caso concreto.

De acuerdo con el contenido del Capítulo V de la LPCU, cuando se trate de operaciones comerciales electrónicas los consumidores tienen derecho a: 1) prácticas equitativas de comercio y publicidad; 2) suministro de información confiable sobre los bienes y servicios ofertados; 3) negarse a recibir mensajes comerciales no solicitados; 4) información especial en el caso de publicidad dirigida a niños, ancianos y personas enfermas; 5) información del proveedor sobre su pertenencia a sistemas de autorregulación; 6) privacidad y confidencialidad de la transacción; 7) protección de datos; 8) corrección de la orden de compra y cancelación de la transacción; 9) seguridad en los medios de pago; 10) especificación de las garantías; y 11) educación al consumidor en materia de comercio electrónico (ARIAS DE RINCÓN, 2005, Nº 6-7). De todos estos derechos, en esta oportunidad nos ocuparemos de la seguridad en los pagos.

La protección relativa al pago

El artículo 40 de la LPCU establece la obligación de proporcionar al consumidor mecanismos fáciles y seguros de pago, información acerca del nivel de seguridad de los mismos, la indicación de las limitaciones al riesgo originado por el uso de sistemas de pago no autorizados o fraudulentos y las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito.

Si se trata de una operación de pago efectuada en el marco del comercio electrónico, el primer apartado del precepto citado exige al proveedor la entrega de la correspondiente factura (que también podría emitirse en formato electrónico), imponiendo además, la obligación de mantener un registro de los pagos con su respectivo respaldo de seguridad durante el tiempo que establezcan las leyes fiscales, luego de la realización de la compra.

La protección establecida en el artículo 40 de la LPCU es complementada con las previsiones del artículo 37 que obliga a los proveedores a utilizar los medios necesarios que permitan la privacidad de los consumidores o usuarios, así como la confidencialidad de las transacciones realizadas.

Del análisis de las normas citadas podemos observar que la mayor preocupación del legislador se centra garantizar la seguridad en los pagos, esta situación se infiere de la propia redacción de las disposiciones en cuestión, la enumeración contenida en el encabezamiento del artículo 40 gira en torno a la seguridad, al exigir información acerca del nivel de seguridad de mecanismos de pago, la indicación del riesgo en sistemas de pago no autorizados o fraudulentos y

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito. Lo mismo podemos decir del artículo 37, que también hace énfasis en la seguridad al establecer la necesidad de garantizar la privacidad y confidencialidad de las transacciones electrónicas.

Consideramos necesario precisar que aun cuando la norma relativa a la protección del pago se encuentra incluida en el Capítulo V de la LPCU, el concepto de pago electrónico no se restringe al ámbito de las operaciones realizadas en el marco del comercio electrónico. Cuando realizamos un pago presencial en el comercio físico tradicional, también podemos estar en presencia de un pago electrónico, tal como sucede con los pagos realizados a través de tarjetas, donde la mecánica operativa del pago exige su verificación en un sistema electrónico (el terminal de punto de venta).

No obstante estas matizaciones, cabe señalar que la expresión utilizada en el encabezamiento del artículo 40 de la LPCU es aún mucho más amplia ya que se refiere a los mecanismos de pago en general, independientemente del calificativo de pago electrónico. No sucede lo mismo con las obligaciones impuestas al proveedor en el primer apartado del precepto citado, donde el legislador alude en forma expresa a los *"… pagos por compras efectuadas en el comercio electrónico".*

Independientemente de las consideraciones expuestas en los párrafos anteriores, en esta oportunidad nos referiremos exclusivamente a la protección del consumidor en las transacciones electrónicas de pago realizadas en entornos abiertos de comunicación, en particular Internet, con especial énfasis en el aspecto de seguridad que es uno de los que más preocupa a los consumidores que realizan operaciones de este tipo.

En relación con los medios de pago consideramos necesario puntualizar que uno de los instrumentos de mayor uso en el comercio en general (presencial y electrónico) es la tarjeta. A pesar de las distintas modalidades existentes en la actualidad (crédito, débito, monederos electrónicos), la tarjeta de crédito es el mecanismo de pago más utilizado en el ámbito del comercio electrónico, de ahí la necesidad de proveer seguridad a este tipo de operaciones. La importancia de este instrumento es tal, que la propia LPCU establece normas de protección específica cuando se trata de pagos materializados a través de tarjetas de crédito. De acuerdo con lo dispuesto en el artículo 40 de la citada ley, cuando el pago se realice mediante una tarjeta de crédito, es necesario indicar las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor del instrumento de pago.

LA SEGURIDAD COMO MECANISMO DE PROTECCIÓN

Como ya indicamos, uno de los aspectos más importantes relacionados con la protección de los consumidores lo encontramos en la obligación establecida en la LPCU de suministrar mecanismos de pago seguros. Para determinar el contenido de este deber, consideramos necesario establecer los requisitos mínimos de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

seguridad que deben rodear las operaciones de pago para entender que éstas son seguras.

En entornos electrónicos, la seguridad en los pagos debe ser estudiada desde un doble aspecto: el técnico y el jurídico. Desde el punto de vista técnico es importante el análisis de los métodos de cifrado de la información, los protocolos de seguridad y otras soluciones que permiten efectuar pagos de forma segura. La seguridad jurídica precisa el estudio de la actuación de cada uno de los sujetos que intervienen en la transacción a efectos de determinar a quién corresponde la responsabilidad en caso de fallos técnicos, violaciones a la privacidad, operaciones no autorizadas o fraudulentas u otras transgresiones en el cumplimiento de los deberes impuestos por normas legales o contractuales.

LA SEGURIDAD TÉCNICA

En la actualidad existen diversos medios para proveer seguridad a las transacciones electrónicas realizadas a través de Internet. Desde el punto de vista técnico, los mecanismos de seguridad los encontramos en la implantación de sistemas criptográficos que permiten el cifrado de la información, en el uso de firmas electrónicas y en los protocolos de seguridad, algunos de ellos diseñados específicamente para proteger los sistemas electrónicos de pago.

De acuerdo con la Norma ISO 7498-92, formulada por la IEC *(International Electrotechnical Commission),* los servicios de seguridad dentro del comercio electrónico deben proporcionar cuatro garantías fundamentales: la autenticación, la integridad, la confidencialidad y el no repudio (tanto en origen como en destino) de los mensajes de datos.

La autenticación se refiere al proceso de verificación de la identidad del remitente del mensaje de datos, esto es, que quien envía el mensaje sea realmente quien dice ser y no otra persona. La autenticación evita supuestos de suplantación de identidad, permitiendo comprobar que los participantes en la operación comercial son quienes dicen ser. Gracias a este servicio, el comprador sabe de modo totalmente seguro en qué comercio está comprando y el proveedor de bienes y/o servicios en Internet puede estar seguro que quien está comprando es realmente el titular del instrumento de pago.

La integridad garantiza que los mensajes son recibidos sin alteraciones no autorizadas, es decir que no han sido modificados, alterados o manipulados durante la transmisión. En materia de pagos efectuados por medios electrónicos, este servicio avala la exactitud de los datos impidiendo que el comprador o el vendedor puedan alegar condiciones diferentes a las pactadas como sería, por ejemplo, una variación en el monto del precio.

La confidencialidad, entendida como el mayor o menor grado de secreto que se adopta sobre una comunicación, garantiza que sólo tengan acceso al mensaje de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

datos quienes estén legítimamente autorizados. En una operación de pago a través de Internet la confidencialidad garantiza el carácter privado de la orden de compra y los datos asociados al instrumento de pago. El servicio de confidencialidad debe entenderse en forma amplia ya que no sólo protege el contenido comercial del mensaje (datos del pedido y de la operación de pago) sino también el acceso a datos de carácter personal por parte de terceros no autorizados.

El no repudio asegura, por una parte, que el emisor, una vez enviado el mensaje, no pueda negar el envío (no repudio en origen) y por la otra, que el destinatario no niegue la recepción ni su contenido (no repudio en destino). El no repudio adquiere singular importancia ya que impide que el comprador niegue el mensaje enviado autorizando el pago a través de su tarjeta u otro instrumento electrónico o que el vendedor niegue hacer recibido el pago.

LA CRIPTOGRAFÍA Y LOS MEDIOS ELECTRÓNICOS DE PAGO

En materia de pagos efectuados a través de medios electrónicos, la criptografía ha adquirido singular importancia en los últimos años, gracias a su implantación en los sistemas de pago propios de las operaciones bancarias y financieras. En el ámbito legal, la criptografía permite dar cumplimiento a la obligación impuesta en el artículo 37 de la LPCU que establece al proveedor el deber de garantizar la confidencialidad de las transacciones realizadas, impidiendo que la información intercambiada sea inteligible para terceros no autorizados que tengan acceso a ella.

En los pagos realizados a través de Internet, la criptografía es una herramienta ideal que proporciona seguridad a la operación, ya que permite ocultar la información que viaja a través de la Red, en estos casos es necesario proteger tanto la información del titular como la información asociada al instrumento de pago. La mayoría de los medios de pago que funcionan en entornos electrónicos se basan en la aplicación sistemas de seguridad que incorporan distintas técnicas de cifrado, unos utilizan criptografía simétrica otros, criptografía asimétrica.

La criptografía simétrica funciona mediante el uso de una clave única, común e idéntica, conocida tanto por el emisor como por el receptor del mensaje, utilizándose ésta para cifrar y descifrar la información. En los sistemas de cifrado asimétrico, el emisor dispone de dos claves matemáticamente relacionadas entre sí: una pública que debe revelar y publicar y otra privada que deben mantener en secreto (Rico Carrillo, 2003, Nº 2). Estos mecanismos de cifrado son muy útiles en los sistemas de pago en Internet ya que permiten la identificación de las partes, a la vez que mantienen la confidencialidad de los datos transmitidos [3].

LOS PROTOCOLOS DE SEGURIDAD

La generalidad en el uso de la tarjeta en Internet, ha motivado el diseño de protocolos de seguridad específicos orientados a proteger los pagos otorgando autenticidad y confidencialidad a la operación, también existen otras soluciones

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

basadas en el empleo de claves secretas y códigos de seguridad asociados al instrumento de pago que aportan seguridad a la transacción [4].

El protocolo SET

Uno de los primeros protocolos diseñado específicamente para proteger los pagos en Internet fue SET *(Secure Electronic Transactions*). Este protocolo fue implementado por las grandes empresas titulares de las marcas de tarjetas (Visa y Masterd Card), con la finalidad de proveer seguridad al pago mediante tarjetas de crédito, gracias a la autenticación de las partes y al mantenimiento de la privacidad de sus datos. Al garantizar la inviolabilidad de los mensajes transmitidos, aporta seguridad a la transacción, impidiendo el acceso a los datos asociados a la tarjeta, su uso fraudulento y la alteración del mensaje.

El mecanismo empleado por SET se basa en el sistema de cifrado doble, el titular cifra el pedido con la clave pública del proveedor de bienes y/o servicios (de manera que sólo pueda ser éste quien descifre el mensaje con su clave privada). La parte referente al pago la cifra con clave pública de la entidad emisora o adquirente según los casos, siendo éstos los únicos que en su caso podrán descifrar esta parte del mensaje mediante la aplicación de su clave privada. El proveedor de bienes al recibir el pedido, remite la orden al emisor quien no tendrá acceso al contenido del pedido pero sí a los datos necesarios para autorizar o denegar la operación, de esta manera se garantiza la confidencialidad de la información (Martín Peña, 2000).

Los niveles de seguridad ofrecidos por SET son bastante altos, aparte de suministrar confidencialidad a la información, garantiza la autenticidad, la integridad y no repudio del mensaje. No obstante la utilidad de este protocolo hemos de destacar que en la práctica comercial no ha tenido mucho éxito, ya que para los usuarios representa un mecanismo complicado al exigir la autenticación de todas las partes y el uso de la firma electrónica.

El protocolo SSL

SSL *(Secure Sockets Layer)* es un protocolo de uso general que facilita el cifrado de la información, la autenticación de servidores, la integridad del mensaje y opcionalmente la autenticación del cliente.

SSL suministra servicios de seguridad en los canales de transmisión entre vendedores y compradores, ocultando los datos intercambiados mediante un algoritmo de cifrado simétrico que proporciona confidencialidad a la operación. A diferencia del protocolo SET, carece de capacidad para verificar la validez del número de tarjeta, autorizar la transacción y procesar la operación con el banco adquirente; su funcionamiento sólo asegura que la información viaja oculta, si alguna persona intercepta el mensaje no podrá acceder a su contenido (Alvarez Marañon, 1999, Nº 156, julio-agosto) (García, 1997, Nº 26). SSL permite dar cumplimiento a la obligación establecida al proveedor en el artículo 37 de la LPCU,

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

de garantizar la confidencialidad de la operación impidiendo que la información transmitida sea accesible a terceros.

El protocolo 3D Secure

Uno de los sistemas de seguridad que más se ha popularizado en el mercado es el protocolo 3D Secure, comercializado bajo las marcas *Verified* de Visa o *Secure Code* de Masterd Card, empresas líderes en el sector de tarjetas de crédito.

Este protocolo permite verificar la identidad del titular de la tarjeta a través de Internet, garantizando la seguridad de la operación. Su funcionamiento se basa en un método de autenticación que usa los mecanismos de cifrado empleados por SSL y un software que es facilitado por el emisor del instrumento de pago. El software se instala en el sitio web del proveedor de bienes y/o servicios y permite la verificación de la identidad del titular, a la vez que protege la información y los datos de la tarjeta durante su transmisión, proporcionando confidencialidad a la transacción.

Para acceder al servicio es necesario darse de alta previamente, para ello, el usuario selecciona una clave secreta y un mensaje de garantía personal que serán utilizados como mecanismos de autenticación. La contraseña de seguridad es distinta del PIN *(Personal Identificación Number*) que se emplea normalmente en las tarjetas, esta clave es denominada CIP (Código Internet Personal) y sirve para que el banco emisor pueda autenticar al titular cuando desee utilizar su tarjeta en Internet.

En el momento de realizar la adquisición del producto o servicio, la tienda se conecta directamente con la institución financiera a efectos de proceder a la autenticación del titular y a la verificación del instrumento de pago. Una vez que se han introducido los datos en el formulario del pedido, se abre la ventana de autorización del pago donde aparece el mensaje personal de garantía que el usuario ha escogido previamente, al comprobar el mensaje, el titular tiene la certeza que es la propia institución financiera la que está realizando el proceso de autenticación y procede a la introducción del CIP. El procedimiento descrito restringe el acceso del proveedor a la operación de pago, situación que le impide conocer los datos de la tarjeta, protegiendo así la confidencialidad de la operación.

Frente a SET, el protocolo 3D ofrece la ventaja que no exige al usuario ningún software especial para su funcionamiento, el sistema es fácil y sencillo de utilizar, ya que sólo se necesita una clave secreta y el número de la tarjeta. En términos del artículo 40 de la LPCU, éste sería un mecanismo de pago fácil y seguro.

LA SEGURIDAD JURÍDICA

La seguridad jurídica se refiere a la protección que otorga el Derecho, la cual se encuentra delimitada en normas de orden legal y/o contractual. En el ámbito jurídico, la protección de las transacciones electrónicas de pago se lleva a cabo

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

mediante el respeto de los derechos de los consumidores y la determinación de la responsabilidad de cada uno de los sujetos que intervienen en la transacción.

En el esquema del funcionamiento de los medios de pago en Internet, uno de los aspectos más importantes de la seguridad jurídica se relaciona con la definición de las obligaciones de las partes a efectos de determinar la responsabilidad ante el incumplimiento de los deberes de cada una de ellas y los posibles fallos que puedan originarse en la transacción, de ahí que el artículo 40 de la LPCU exija la indicación de las limitaciones del riesgo originado por el uso de sistemas de pago no autorizados o fraudulentos, así como las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito.

LA IMPORTANCIA DEL CONTRATO EN EL ESQUEMA DEL PAGO ELECTRÓNICO

En la actualidad son escasas las normas que se encargan de establecer el régimen jurídico aplicable a las tarjetas, muy pocos los países cuentan con leyes especiales en esta materia. La fuente generadora de obligaciones la encontramos en las relaciones contractuales que se establecen entre los sujetos que participan en el mecanismo de pago, de ahí su importancia.

Los sujetos que intervienen en el esquema del pago con tarjetas son básicamente tres: la entidad que emite o gestiona el medio de pago, el proveedor de bienes y/o servicios y el titular. En las operaciones en Internet, también es importante la actuación de los intermediarios que prestan servicios de acceso a cada uno de los sujetos que participan en la transacción.

Las partes involucradas en el mecanismo del pago se vinculan entre sí a través una relación triangular que se articula sobre la base de distintos contratos. Entre el titular y el emisor existe un contrato de emisión; entre el aceptante y el emisor, un contrato de aceptación o afiliación; y entre el titular y el aceptante un contrato de cambio que origina la obligación de pago.

En Europa, el contenido del contrato de emisión ha sido objeto de regulación en varias recomendaciones emanadas de la Comisión Europea, de todas ellas destaca la Recomendación de la Comisión 97/489, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos [5]. En el marco de este instrumento se recomienda el establecimiento de requisitos mínimos de información que deben cumplirse en el momento de fijar las condiciones aplicables a las transacciones efectuadas mediante instrumentos electrónicos de pago, así como las obligaciones y responsabilidades mínimas de las partes involucradas.

En Venezuela, la LPCU también contempla el deber de información al exigir que se indiquen las limitaciones del riesgo y las medidas de corresponsabilidad entre el

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

proveedor y el emisor de la tarjeta, estas indicaciones deben estar determinadas tanto en los contratos que vinculan a estos sujetos entre sí (contratos de afiliación) como en el contrato que existe entre el titular del instrumento de pago y el emisor (contrato de emisión); el incumplimiento de los deberes contractuales genera responsabilidad por los daños y perjuicios causados.

OBLIGACIONES DE LAS PARTES INVOLUCRADAS EN EL MECANISMO DEL PAGO

Las obligaciones de los sujetos que intervienen en el mecanismo del pago electrónico se encuentran delimitadas en los respectivos acuerdos contractuales. Es necesario conocer los deberes de cada uno de ellos a efectos de poder atribuir responsabilidad en el caso de operaciones no autorizadas o fraudulentas, tal como lo establece la LPCU.

El contrato de emisión faculta al titular para usar legítimamente el instrumento de pago. Mediante este contrato, el titular se obliga al uso adecuado de la tarjeta y a la custodia, tanto del instrumento físico como de la clave secreta (PIN), asumiendo el deber de notificar al banco la pérdida o el uso no autorizado. El cumplimiento de las obligaciones impuestas al titular adquiere especial importancia en el momento de determinar la responsabilidad ante usos fraudulentos, ya que una infracción de parte de éste a los deberes que impone la utilización del medio de pago puede traducirse en una causa de exoneración de responsabilidad para las demás partes involucradas.

Frente al titular, el emisor se obliga a la emisión y gestión del medio pago, al suministro de información respecto del funcionamiento del instrumento y al registro de las operaciones realizadas por el titular, que normalmente se refleja en los estados de cuenta accesibles a través de la página web de la institución. También se obliga a disponer de un sistema de atención al cliente que facilite la notificación por pérdida y la inutilización de la tarjeta mediante el bloqueo de las operaciones de pago.

El contrato de afiliación define los derechos y obligaciones entre los proveedores de bienes y/o servicios y los emisores, por virtud de este contrato, el proveedor se obliga a aceptar la tarjeta como medio de pago en las transacciones que realice el titular, asumiendo la obligación de verificar la validez del instrumento, comprobar la legitimación del titular con la confrontación del documento de identidad y verificar que la firma estampada en el impreso que expide el terminal de punto de venta (TPV), coincida con la que se encuentra en la cara posterior de la tarjeta.

Frente al aceptante, el emisor se obliga al pago de las facturas firmadas por el titular y a la instalación de los mecanismos técnicos que permiten gestionar la autorización de la transacción, el tradicional TPV de los comercios físicos o las pasarelas de pago o TPV virtuales, propios de las operaciones comerciales electrónicas.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

LA OBLIGACIÓN DE SUMINISTRAR PAGOS SEGUROS

Como ya indicamos, el artículo 40 de la LPCU establece la obligación de suministrar al consumidor mecanismos de pago, fáciles y seguros, exigiendo la información acerca del nivel de seguridad de los mismos. Esta información debe contener las limitaciones del riesgo originado por el uso de sistemas de pago no autorizados o fraudulentos, así como las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito.

La disposición se refiere a tres situaciones específicas: la indicación de las limitaciones del riesgo, las medidas de reembolso y la responsabilidad que debe imputarse al proveedor o al emisor, o a los dos en conjunto, si el fuera el caso. En esta oportunidad nos ocupamos del estudio de la determinación del riesgo y la responsabilidad, en el entendido que el reembolso de la operación corresponderá a quien se atribuya la responsabilidad.

La indicación del riesgo y la determinación de responsabilidad en caso de operaciones no autorizadas o fraudulentas

Las limitaciones del riesgo derivadas del uso de la tarjeta deben estar especificadas en los contratos asociados al instrumento de pago, recordemos que existe una relación triangular que se articula en los contratos de emisión y aceptación de la tarjeta. En cuanto a la atribución del riesgo en caso de operaciones no autorizadas o fraudulentas ¿Quién debe asumir el riesgo? ¿El aceptante? ¿El emisor? ¿El titular? Para dar respuesta a estas interrogantes será necesario analizar la diligencia empleada por cada una de las partes en el cumplimiento de sus deberes a objeto de establecer la responsabilidad correspondiente.

En principio, el emisor es responsable frente al titular por las transacciones no autorizadas o fraudulentas, sin embargo, en estos casos es necesario determinar la diligencia del titular en el cumplimiento de la obligación de notificar la pérdida o robo del instrumento, ya que el incumplimiento de tal deber puede exonerar de responsabilidad al emisor. También debe analizarse la actuación del aceptante en relación con la diligencia empleada en el proceso de verificación la identidad del titular y la validez del instrumento de pago, si el aceptante no ha cumplido diligentemente esta obligación, debe asumir la responsabilidad por la operación no autorizada o fraudulenta. El principal problema que se presenta en las operaciones de pago en Internet, lo encontramos en la dificultad de comprobar la identidad de la persona que está utilizando el medio de pago.

Los pagos realizados en el comercio electrónico en Internet difieren de los pagos realizados en el comercio tradicional por la falta de presencia física de las partes, en estos casos, el aceptante tiene que emplear medios de comprobación diferentes de los que normalmente usa en las operaciones tradicionales. Para verificar la identidad del titular se utilizan mecanismos basados en el suministro de claves personales y códigos de seguridad asociados al instrumento de pago, también los

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

protocolos de seguridad descritos anteriormente y, en menor medida, firmas electrónicas basadas en criptografía de clave pública.

Para comprobar la validez de la tarjeta se utilizan pasarelas de pago que son instaladas por el emisor y gestionadas por él mismo o por un tercero, es de destacar que el mecanismo de la pasarela de pagos sólo permite la verificación técnica del instrumento de pago (que no esté vencido, anulado o que la operación no exceda del límite de crédito autorizado), el sistema no puede garantizar que sea el propio titular quien está efectuando la operación. En estos casos, la responsabilidad del emisor se circunscribe al funcionamiento técnico de la pasarela de pagos, sin responder de la identidad del sujeto que está utilizando la tarjeta. Esta circunstancia debe estar especificada en los contratos de afiliación, aquí nos encontramos con un ejemplo de delimitación del riesgo, el emisor, al exonerarse de responsabilidad por la verificación de la identidad del titular traslada el riesgo de las operaciones fraudulentas al aceptante.

En el caso de operaciones no autorizadas o fraudulentas el titular tiene el derecho de anular el cargo, siempre, claro está, que haya cumplido su obligación de notificar la pérdida o robo del instrumento, esta situación se encuentra prevista en los respectivos contratos de emisión, aquí podemos ver otro ejemplo de delimitación de riesgo y responsabilidad. Es de destacar que artículo 40 de la LPCU no consagra en forma expresa el derecho de anulación del cargo, sin embargo, siempre que se trate de operaciones de este tipo el titular tiene tal derecho y para hacerlo efectivo debe presentar su reclamación ante el emisor, que es el responsable de autorizar la transacción.

Luego habrá que determinar la actuación del aceptante y su correspondiente responsabilidad por la operación realizada, ya que un incumplimiento en su deber de comprobación puede dar lugar a una operación no autorizada o fraudulenta, de ahí que el artículo 40 de la LPCU insista en la corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito. Una vez que el titular ha solicitado la anulación del cargo, el emisor procede a reversar la operación y detraer el importe que se había abonado en la cuenta del aceptante.

Según las consideraciones expuestas, en los pagos realizados en el comercio electrónico, el riesgo de las operaciones fraudulentas finalmente va recaer sobre el aceptante (proveedor), que es quien sufre la pérdida económica una vez que se efectúa el reverso de la operación. Como ya indicamos, la delimitación del riesgo en este tipo de operaciones debe estar especificada en los contratos de afiliación. Las cláusulas que eximen de responsabilidad al emisor y atribuyen el riesgo de la operación al proveedor son muy comunes en este tipo de contratos, la jurisprudencia española ha declarado la validez de estas cláusulas entendiendo que el riesgo de la operación lo debe asumir el aceptante, ya que es él quien *"…decide efectuarlas bajo su propio riesgo, en el entendido que deberá aceptar el adeudo del importe si el emisor de la tarjeta que figura como utilizada no admite el cargo de su operación…"* [6]. En este escenario, viene a ser el proveedor de bienes y/o servicios

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

aceptante del medio de pago, la persona más interesada en la implementación de mecanismos de seguridad.

El cumplimiento del deber de información respecto al nivel de seguridad

De acuerdo con el artículo 40 de la LPCU, el suministro de pagos seguros debe incluir información acerca del nivel de seguridad. Como se analizó anteriormente, existen distintos tipos de mecanismos para proveer seguridad a las operaciones de pago, unos aportan mayor seguridad que otros. Es de destacar que La LPCU no impone exigencias determinadas en cuando a parámetros de seguridad, sólo establece el deber de informar al consumidor acerca del nivel de seguridad, tampoco dice la ley el sitio donde debe constar tal información.

Al tratarse de mecanismos técnicos de seguridad, lo normal que esa información se encuentre en las condiciones generales incluidas en las páginas web de los proveedores de servicios; también es común que este tipo de información se haga accesible a los usuarios durante el proceso de compra, la mayoría de los sitios web que cuentan con mecanismos de seguridad incorporan en el funcionamiento del sistema una ventana que indica el nivel de confianza de la página.

El deber de información debe incluir las limitaciones al riesgo en caso de operaciones no autorizadas o fraudulentas y las medidas de reembolso o corresponsabilidad entre el proveedor y el emisor de tarjetas de crédito. Como vimos en los apartados anteriores, esa información normalmente está incluida en los contratos que rodean las operaciones de tarjeta, es importante mencionar que las limitaciones al riesgo casi siempre se encuentran determinadas en las condiciones generales de contratación que se incorporan a los contratos de emisión y aceptación.

En muchos casos estas cláusulas se configuran como abusivas en perjuicio de los consumidores y usuarios, al estar redactadas por los propios emisores de tarjetas es normal que ellos pretendan exonerarse totalmente de los riesgos de la transacción, aún por el funcionamiento de los sistemas técnicos instalados para el procesamiento de los pagos. Esta materia también es objeto de tutela en la LPCU, una cláusula que permita la exención total de responsabilidad por el funcionamiento técnico de la pasarela de pagos sería inválida, ya que configura uno de los supuestos de nulidad establecidos en el artículo 87 de la LPCU.

Los sujetos obligados al cumplimiento de la obligación

El artículo 40 de la LPCU no indica quién debe cumplir la obligación de suministrar pagos seguros, su formulación textual es la siguiente: "*A los consumidores se les deberá proporcionar mecanismos fáciles y seguros de pago*". Como podemos ver, la norma no específica quién es el titular de la obligación, en principio y según las consideraciones expuestas anteriormente, el deber de suministrar mecanismos de seguridad en los pagos corresponde tanto al proveedor

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

como al emisor. Aun cuando el riesgo de la operación es soportado en la mayoría de las veces por los proveedores, los emisores también deben responder por la seguridad en los sistemas de pago, recordemos que el propio artículo 40 consagra un sistema de corresponsabilidad entre proveedores y emisores en favor del titular.

El emisor es responsable por la seguridad en el funcionamiento técnico de los sistemas instalados para procesar los pagos (los TPV o las pasarelas de pago). También debe responder por el suministro de información acerca de los niveles de seguridad sobre el uso de los medios de pago que ha proporcionado al titular, particularmente en el caso de operaciones realizadas a través de Internet. En relación con los proveedores, la responsabilidad en el cumplimiento de su obligación se centra en la instalación de sistemas que permitan la confidencialidad de la transacción y la identificación del consumidor a objeto de evitar las operaciones no autorizadas o fraudulentas y en el deber de información acerca del nivel de seguridad de los mecanismos empleados (Arias de Rincon, knlxn).

LA CONFIDENCIALIDAD DE LA OPERACIÓN

Uno de los aspectos que más preocupa a los usuarios de la Red es la falta de confidencialidad de la operación, debido a la facilidad que ofrece el sistema para la interceptación del mensaje por terceras personas, quienes pueden tener acceso a datos personales y a la información del instrumento de pago y usarla con fines ilícitos [7]. En Venezuela, la necesidad de suministrar confidencialidad a las transacciones electrónicas se encuentra prevista en el artículo 37 de la LPCU al exigir al proveedor la obligación de utilizar mecanismos que garanticen la privacidad de los consumidores, *"…así como la confidencialidad de las transacciones realizadas, de forma tal que la información intercambiada no sea inteligible para terceros no autorizados que tengan acceso a ella voluntaria o accidentalmente".*

La confidencialidad de la operación se encuentra directamente relacionada con el derecho a la privacidad y la protección de datos de carácter personal, aunque el artículo 40 de la LPCU no se refiera en forma expresa a la confidencialidad de las transacciones de pago, es una garantía que también debe proporcionarse a los consumidores. Las operaciones electrónicas no sólo permiten la captación de datos por parte de terceras personas, los sujetos involucrados en el mecanismo del pago (entidades financieras, comerciantes, intermediarios) también pueden captar información personal y del instrumento de pago (números de tarjetas, passwords, cuentas bancarias) y utilizarla con fines ilícitos. Esta situación también facilita el tratamiento de datos, que en la mayoría de los casos se realiza sin el consentimiento del titular.

Desde el punto de vista técnico, la confidencialidad de las operaciones en Internet se consigue mediante el uso de los protocolos de seguridad basados en técnicas criptográficas que permiten ocultar la información, descritos anteriormente. En el ámbito jurídico cada vez es más frecuente la adopción de normas

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

encaminadas a regular el tratamiento de datos personales y garantizar la privacidad en las transacciones electrónicas.

En Venezuela no existe en la actualidad una ley especial destinada a garantizar la protección de datos de carácter personal, ello no quiere decir que los consumidores se encuentren totalmente desprotegidos en este aspecto, ya que el artículo 38 de la LPCU establece una protección especial para el caso del tratamiento de datos en las operaciones comerciales electrónicas. La disposición citada impone al proveedor el deber de otorgar al consumidor la posibilidad de escoger, entre la información recolectada, aquella que no podrá ser suministrada a terceras personas.

De acuerdo con las previsiones contenidas en los artículos 37 y 38 de la LPCU, la obligación de garantizar la privacidad y confidencialidad de la operación compete al proveedor, quien debe asumir la responsabilidad frente al consumidor en caso de trasgresión en el cumplimiento de tal deber.

CONCLUSIONES

1. La seguridad en los medios de pago es uno de los elementos fundamentales para el desarrollo del comercio electrónico en Internet. En Venezuela, las normas sobre protección de los consumidores en las transacciones de pago se encuentran incluidas en el Capítulo V de la Ley de Protección al Consumidor y Usuario. La mayor preocupación del legislador en este aspecto, se centra en garantizar la utilización de mecanismos de pago seguros.

2. A efectos de establecer el contenido de la obligación de suministrar pagos seguros es necesario determinar los requisitos de seguridad, tanto técnicos como jurídicos que deben estar presentes en la operación de pago para considerar que se han cumplido las normas de protección de los derechos de los consumidores.

3. Desde el punto de vista técnico, los mecanismos de seguridad permiten la autenticación, integridad, confidencialidad y no repudio del mensaje. En la actualidad existen diversos protocolos y mecanismos que aportan distintos niveles de seguridad a las operaciones de pago. En el ámbito jurídico es necesario determinar el régimen de responsabilidad de las partes que intervienen en el mecanismo de pago, lo cual exige que las obligaciones estén claramente delimitadas. La determinación se lleva a cabo a través de los contratos que vinculan a cada uno de los participantes de la operación de pago.

4. El deber de suministrar mecanismos de pago seguro incluye la información acerca del nivel de seguridad, la indicación de las limitaciones del riesgo por operaciones no autorizadas o fraudulentas y las medidas de reembolso o corresponsabilidad entre proveedores y emisores. La LPCU no especifica quién es el sujeto obligado al cumplimiento de tal deber, esto implica estas obligaciones

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

deben ser satisfechas tanto por los proveedores como por los emisores de los medios de pago electrónicos.

5. Aunque el artículo rector en materia de pagos no se refiera en forma expresa a la confidencialidad de la operación, esta garantía también debe proporcionarse a los consumidores, en el entendido que uno de los aspectos que más preocupa a los usuarios de Internet es falta la confidencialidad en la operación de pago. Sobre este aspecto consideramos de aplicación al pago la norma incluida en el artículo 37 de la LPCU, que establece la obligación al proveedor de garantizar la utilización de medios que permitan la privacidad así como la confidencialidad de las transacciones realizadas.

6. Desde el punto de vista técnico, los problemas relacionados con la confidencialidad en los pagos se solucionan con el auxilio de la criptografía y otros mecanismos que permiten ocultar la información. En el ámbito jurídico, destaca la tutela que ofrecen las normas de protección de datos de carácter personal, aunque en Venezuela no existe regulación especial en esta materia, los derechos de los consumidores en relación con la circulación de datos de carácter personal en las operaciones electrónicas son objeto de protección en el marco de la LPCU.

NOTAS

[1] En Europa, la Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre Comercio Electrónico y Servicios Financieros, pone de manifiesto la necesidad de desarrollar medidas que garanticen el uso de sistemas de pago seguros. En este mismo sentido se ha pronunciado el Banco Central Europeo en el Informe sobre Dinero Electrónico de agosto de 1998, donde se destaca la importancia de proveer mecanismos de pago seguros para lograr la confianza en los medios electrónicos de pago.

[2] Publicada en la Gaceta Oficial No. 37.930, de 04 de mayo de 2004.

[3] En el Informe sobre Dinero Electrónico del Banco Central Europeo de 1998, se menciona la criptografía como el medio idóneo para autenticar las transacciones y proteger la confidencialidad e integridad de la información en los productos de dinero electrónico

[4] El CCV (*Credit Card Verificación*) es un mecanismo de seguridad implementado con la finalidad de facilitar la autenticación del titular del instrumento de pago en las operaciones a través de Internet. Se trata de un número compuesto por tres dígitos que normalmente se encuentra impreso en el lado posterior de la tarjeta, en el campo designado para la firma del titular. Aun cuando este método contribuye a aportar seguridad a la operación, sólo permite al proveedor asegurarse que la persona que está comprando tiene en su poder la tarjeta, el mecanismo no garantiza que sea el propio titular el que está efectuando la operación, ya que al encontrarse el CCV impreso en el propio instrumento de pago, puede ser utilizado por cualquier persona que haya obtenido la tarjeta.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007

[5] Diario Oficial de las Comunidades Europeas No. L 208/52 de 2 de agosto de 1997

[6] Sentencia del Juzgado de 1ª Instancia nº 7 de Donostia-San Sebastián de 13 de octubre de 2004.

[7] En España, el Estudio sobre Comercio Electrónico B2C de 2005, realizado por La Entidad Pública Empresarial Red.es, determinó que existe un número considerable de personas que se abstienen de comprar en Internet. Las principales razones expuestas por los consumidores fueron la desconfianza en el pago y el miedo a enviar datos personales a través de la Red. Los resultados de este estudio se encuentran disponibles en Internet, vid. Ministerio de Industria, Comercio y Turismo de España, Estudio sobre Comercio Electrónico B2C 2005, p. 10 (http://observatorio.red.es/estudios/documentos/estudio%20_b2c_2005.pdf).

REFERENCIAS BIBLIOGRÁFICAS

Alvarez Marañon, G. (1999, Nº 156, julio-agosto). Medios de pago en Internet: cómo comprar inteligentemente . *PC World* , 224.

Arias de Rincón, M. I. (Nº 6-7). La protección al consumidor en el comercio electrónico . *Derecho y Tecnología* , 53-71.

García, M. (1997, Nº 26). Autenticación y cifrado para un comercio electrónico seguro. *SIC* , 51-52.

Martín Peña, R. (2000). Exposición de una operación de comercio electrónico seguro con una tarjeta bancaria. *XIII Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia de Comillas* , 115-120.

Rico Carrillo, M. (2003, Nº 2). Firmas electrónicas y criptografía. *Derecho y Tecnología* , 81-104.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 6 Edición No 3 – Año 2007