

Estudio Jurídico sobre el impacto del fraude



Análisis comparativo de normativa europea, cláusulas y prácticas abusivas

Los fraudes en medios de pago: una amenaza para la economía de los consumidores europeos

Organiza:



ADICAE
Asociación de Usuarios
de Bancos, Cajas y Seguros

Con la colaboración de:



**DG JUSTICIA, LIBERTAD
Y SEGURIDAD**
Comisión Europea



Edita:

ADICAE

Asociación de Usuarios de Bancos, Cajas y Seguros

Servicios Centrales

c/ Gavín, 12 local - 50001 Zaragoza

Tel.: 976 39 00 60

Fax: 976 39 01 99

email: aicar.adicae@adicae.net

www.adicae.net

Índice

PRESENTACIÓN

- Los fraudes en medios de pago: una amenaza para la economía de los consumidores europeos 3

PARTE 1. FRAUDES Y MEDIOS DE PAGO: UNA COMBINACIÓN DEMASIADO HABITUAL QUE AFECTA A LA SEGURIDAD DE LOS CONSUMIDORES

1. *Medios de Pago*: los consumidores ya no pagan sólo con dinero 7
2. El “*Fraude*”, un delito contra los intereses económicos de los usuarios 12
3. Clases de fraude en Medios de Pago y sus consecuencias para el consumidor 14

PARTE 2. RETOS Y DEFICIENCIAS DE LA NORMATIVA EUROPEA EN LA PROTECCIÓN DEL CONSUMIDOR ANTE EL FRAUDE EN MEDIOS DE PAGO

1. Medidas contra el fraude en la Unión Europea: control de contratos, fijación de responsabilidades y prevención 18
2. Normativa Europea sobre tipos penales comunes y cooperación judicial frente al fraude en medios de pago 29

PARTE 3. LA REGULACIÓN Y CONTROL PENAL EN ESPAÑA: LUCES Y SOMBRAS EN LA LUCHA CONTRA EL FRAUDE EN MEDIOS DE PAGO

1. La regulación penal española del fraude en medios de pago: demasiada confusión 39

PARTE 4. LAS MALAS PRÁCTICAS Y CONDICIONES ABUSIVAS DE BANCOS Y CAJAS CON RELACIÓN A LOS MEDIOS DE PAGO

1. Análisis de las malas prácticas de las entidades en medios de pago: fraudes que se repiten año tras año 61
2. Cláusulas abusivas en los contratos de medios de pago: abundantes y sin control previo 64

PARTE 5. PROBLEMAS EN MEDIOS DE PAGO Y AUSENCIA DE PROCEDIMIENTOS DE RESOLUCIÓN RÁPIDOS Y EFICACES: UNA EXIGENCIA PARA LOS DERECHOS DE LOS CONSUMIDORES

1. Consumidores y resolución extrajudicial de conflictos en servicios financieros. Situación actual, perspectivas y propuestas 69

CONCLUSIONES Y PROPUESTAS:

- El mercado único de los medios de pago necesita de la seguridad y confianza de los consumidores y la participación en su diseño de sus asociaciones 74

ANEXO 1. SENTENCIAS JUDICIALES SOBRE FRAUDES EN MEDIOS DE PAGOS	78
ANEXO 2. NORMATIVA SOBRE FRAUDE EN MEDIOS DE PAGO EN PAÍSES PARTNERS Frente a los fraudes en medios de pago, la normativa de los distintos países europeos necesita cohesión	89
ANEXO 3. RESOLUCIÓN EXTRAJUDICIAL DE CONFLICTOS EN EUROPA (PAÍSES PARTNERS) El acceso a la justicia en Europa	92
ANEXO 4. RESUMEN DE LA NORMATIVA EUROPEA	108

Los fraudes en medios de pago: una amenaza para la economía de los consumidores europeos

En las economías modernas, los sistemas y los instrumentos de pago constituyen un elemento fundamental para la economía real. Las operaciones de pago perfeccionan las operaciones de compraventa o de prestación de servicios, siendo un aspecto fundamental para los consumidores. Unos sistemas y proveedores de pagos sanos contribuyen a la confianza en la estabilidad financiera de un país, pero además, cabe exigirles que para los consumidores generen confianza en la seguridad que realizan a través de esos pagos: a menor fraude, mejora la confianza de los usuarios y, por tanto, el desarrollo de un mercado interno sin trabas del que los consumidores son pieza clave para su constitución efectiva.

En la búsqueda de sistemas de pago eficientes, muchas entidades financieras se han orientado hacia la adopción de sistemas de pagos electrónicos. En efecto, cuando hablamos de “medios de pago distintos del efectivo”, nos estamos refiriendo a la gran evolución que se ha producido en este ámbito merced a los avances tecnológicos. Así, podemos diferenciar entre medios de pago tradicionales, tales como letras de cambio, cheques, pagarés; y los modernos medios de pago como la transferencia, el pago con tarjeta, el dinero electrónico, etc. Se aprecia una reducción en la importancia de los medios de pago tradicionales mientras que los pagos electrónicos van ganando relevancia, lo que redundará en rapidez en la prestación del servicio de pago.

No obstante, lo que produce oportunidad de mejora en la prestación de un servicio, provoca también riesgos para quien hace uso del mismo. El potencial de las nuevas tecnologías no está dando una solución satisfactoria a los graves problemas que para los consumidores plantea el fraude en estas operaciones. Por un lado, la debilidad de muchos sistemas operativos (clonación de bandas magnéticas en tarjetas, robo de datos bancarios a través de Internet, etc.) están demostrando que la tecnología no ofrece una respuesta justa para reducir a la mínima expresión posible estos riesgos. No parece que las propias entidades financieras que ponen en el mercado esos instrumentos de pago garanticen un adecuado nivel de protección a sus clientes, mediante una política de inversión en seguridad y nuevas tecnologías adecuada. Al contrario, son en muchas ocasiones las propias entidades quienes hacen recaer en el usuario toda la responsabilidad por la comisión de estos fraudes, eximiéndose de responsabilidad y haciendo recaer sobre la parte más débil de la relación (los consumidores) todas las consecuencias de los fraudes.

Si las nuevas tecnologías no logran dar una respuesta todavía suficiente ante los riesgos de fraude, la legislación que regula su uso tampoco ha contribuido a paliarlos. Antes bien, ha contribuido a la indefensión e inseguridad de los propios usuarios permitiendo “normativas blandas”, en forma de Recomendaciones Europeas, que ha generado Códigos de Conducta o cláusulas contractuales donde la posición del usuario de medios de pago sale notoriamente debilitada. Si el nivel tecnológico no permite una respuesta segura al cien por cien, debe al menos existir una legislación clara y garante con los derechos de los consumidores que resuelva de forma justa problemas derivados del fraude como la responsabilidad en caso de comisión, una responsabilidad que no podría recaer exclusivamente en la parte más débil, como hasta ahora hacen muchas entidades financieras.

El legislador europeo y los respectivos reguladores estatales, así como las entidades emisoras y prestadoras de estos servicios deben ser conscientes de estas necesidades, y de que un mercado interior único en medios de pago exige ganarse la confianza de los consumidores. En este sentido se manifiesta el reciente Dictamen del Comité Económico y Social Europeo de 30 de abril de 2009 sobre “La lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo”, que expresamente reconoce que “una acción eficaz de lucha contra el fraude facilitaría la creación de la SEPA (espacio único de pagos en Euros)”.

Todas estas cuestiones, y otras muchas más, se han planteado en el Proyecto encabezado por ADICAE, “Seminario sobre Fraudes en Medios de pago en la Unión Europea”, que ha reunido a 9 asociaciones de consumidores de 7 países europeos diferentes (República Checa, Italia, Lituania, Rumanía, Eslovaquia, Eslovenia y Bulgaria). Este proyecto, que tiene como

finalidad la prevención del fraude en medios de pago, persigue mejorar la asociación entre el sector público y el privado, la cooperación con los sistemas judicial, penal y policial, asociaciones de consumidores y otras entidades profesionales para así desarrollar estrategias e instrumentos para combatir la delincuencia en el sector de medios de pago electrónico, aumentando la cooperación y la coordinación entre los actores competentes a nivel europeo.

Una de las herramientas fundamentales para dar cumplimiento a estos objetivos es la elaboración de un Estudio jurídico sobre el fraude en medios de pago distinto de efectivo, evaluando la normativa dictada desde las Instituciones Europeas y de los distintos países miembros participantes del Proyecto. Analizar los problemas jurídicos que plantean a los consumidores el uso fraudulento en los medios de pago exige conocer la tipología de estos fraudes, las consecuencias para los legítimos intereses económicos de los consumidores y evaluar las respuestas de la normativa actual.

Un Estudio de estas características no podría quedar completo de forma satisfactoria sin una serie de propuestas concretas de mejora, cuya inclusión en la normativa y actuación de entidades públicas y privadas contribuiría, sin duda a paliar la grave posición de desequilibrio de los consumidores frente al fraude en los medios de pago. Sólo mediante estrategias e instrumentos técnicos y jurídicos eficaces, puede lograrse una mayor seguridad en el sistema que genere la confianza necesaria en millones de personas que cada vez más utilizan y utilizarán medios de pago electrónico en la Unión Europea. Pero también es importante mejorar la colaboración entre Administraciones públicas y empresas prestadoras de este servicios, por un lado, con las Asociaciones de Consumidores Europeas de otro.

ADICAE siempre ha actuado en defensa de los intereses de los usuarios de medios de pago en su interés por proteger los derechos de los consumidores. Desde 2005 ha participado activamente en diversos encuentros organizados por el Grupo de Medios de Pago de la Comisión Europea, con la finalidad de impulsar en Europa un área de pago unificado mediante la implantación del SEPA (Single Euro Payments Area), cuyo objetivo es extender al ámbito de los pagos electrónicos la unidad monetaria efectiva que ya existe en el ámbito de monedas y billetes. Asimismo ADICAE ha formado parte del Grupo de Trabajo para la prevención de Fraudes en Medios de Pago de la Dirección General de Mercado Interior de la Comisión Europea.

D. Manuel Pardos. Presidente de ADICAE

Parte 1

Fraudes y medios de pago: una combinación demasiado habitual que afecta a la seguridad de los consumidores

El desarrollo tecnológico en el mundo de los medios de pago ha propiciado que el pagar con efectivo cada vez se haga más inusual. Tarjetas electrónicas, cheques, transferencias, incluso el pago por móvil, entre otros, están desplazando al dinero en efectivo. Esto supone un gran avance, mucho más cómodo para ambas partes, pero a su vez hacen necesario que quienes utilizan un medio de pago diferente del efectivo conozcan su funcionamiento, sus particularidades y carencias o posibles vulnerabilidades ante el fraude, puesto que ninguno de los medios de pago existentes es totalmente seguro.

A la hora de encarar un análisis jurídico sobre fraude en medios de pago requiere definir y delimitar previamente el ámbito sobre el que va a realizarse dicho análisis. Vamos a centrar la cuestión en primer lugar respecto de los “medios de pago”, y posteriormente se analizará la noción de “fraude”, relacionándola con los modernos sistemas de pago y su variada tipología a disposición de los consumidores europeos. Abordar esta idea al igual que definir qué es el fraude y las clases de fenómenos que se dan dentro de éste son fundamentales para analizar posteriormente la normativa existente en este tema, piedra angular de este Estudio.

Para finalizar, también se abordan las consecuencias que tiene el fraude para el usuario en sus derechos económicos, en la mayoría de las ocasiones son consecuencias desfavorables, puesto que las entidades financieras en los contratos de estos medios de pago derivan todas estas consecuencias hacia el consumidor.

Medios de Pago: los consumidores ya no pagan sólo con dinero

Entendemos por “medio de pago” todo instrumento material (exceptuada la moneda de curso legal), que por su naturaleza específica permita, por sí sólo o junto con otro instrumento, al titular o usuario transferir dinero o un valor monetario y que esté protegido contra las imitaciones o la utilización fraudulenta. Esta descripción descarta no sólo el dinero en efectivo (billetes y monedas de curso legal) sino también el dinero electrónico en sentido estricto al carecer de soporte material. En la práctica cotidiana los “medios de pago” utilizados de manera mayoritaria son herramientas que tienen un componente tecnológico avanzado. Figuras como el cheque, el pagaré o la letra de cambio, si bien se consideran a efectos de esta noción como “medios de pago distintos del efectivo”, no cabe duda de que, o bien están en desuso (con excepción quizá del cheque), o bien su empleo predominante se impone en operaciones entre empresas (pagaré).

Los medios de pago más difundidos tienen un componente tecnológico complejo

Es precisamente el componente tecnológico el que condiciona su uso y sus consecuencias por varias razones. En primer lugar, porque tales tecnologías permiten una operatividad en tiempo y espacio enormemente rápida y que, incluso, supera las fronteras entre estados (transferencias). Pero a su vez, conlleva un componente de riesgo alto que afecta a los consumidores, como tendremos ocasión de comprobar. Los medios de pago con un alto componente tecnológico, o utilizados en medios con elevado nivel de aplicación tecnológica (servicios de banca electrónica a través de internet), son hoy día un reto para la seguridad de los intereses legítimos de los consumidores y exigen que el esfuerzo de este Estudio se centre en esta dirección.

A continuación expondremos una relación donde se analizan las características de los medios de pago distintos del efectivo, que responden por tanto a la definición planteada, que son los más habituales y empleados por el consumidor.

1. Las tarjetas electrónicas, el medio de pago más común y problemático entre los consumidores

En los últimos años, la circulación de tarjetas bancarias ha pasado de cuarenta millones a superar los setenta millones de tarjetas emitidas, según datos del Banco de España en 2008. Se trata de un sistema de pago electrónico que, además, se viene aplicando de forma generalizada como medio de pago en el comercio electrónico. Es el medio de pago más utilizado para operar por Internet como tendremos oportunidad de conocer, con los problemas que ello conlleva.

En particular, la tarjeta bancaria es el medio de pago electrónico generado a través de un documento emitido por bancos y cajas de ahorro sobre todo, pero también por grandes almacenes y otras entidades, que permite a su titular el pago sin dinero en efectivo o el acceso al cajero automático. El titular de la tarjeta abona una serie de bienes y/o servicios, con cargo a la cuenta abierta o asociada a la tarjeta que tiene con la entidad emisora de la misma.

Seguridad en el uso de las tarjetas a través de Internet: un aspecto conflictivo

Las tarjetas permiten también el pago en las compras realizadas a distancia y también en las realizadas a través de Internet (“on-line”), si bien la seguridad de la transacción para el consumidor requiere la existencia de un certificado SET (Secure Electronic Transactions – Transacciones electrónicas seguras).

Para garantizar la confidencialidad en el envío de información sensible a través de la Red Internet, se ha impuesto como estándar el protocolo de seguridad “SSL”. Se trata de un sistema de cifrado de datos prácticamente inexpugnable, si bien no evita que alguien haga uso de una tarjeta ajena, pues sólo garantiza que nadie se interpondrá entre el comprador y el vendedor en el proceso de pago. Por esta razón se desarrollan otros sistemas que solicitan una clave al introducir el número de la tarjeta para garantizar la identidad del comprador. Este es precisamente el sistema de certificado “SET”, que a su vez está siendo sustituido por el sistema “3D Secure”, en el que se basa el estándar internacional de Comercio electrónico Seguro (CES) desarrollado por “Visa” y por “Mastercard” y ofrecido por las entidades financieras y bancarias (incluidas las cajas de ahorro). Con todo, el uso de estos sistemas de seguridad de pago en la red mediante el uso de tarjeta de crédito todavía no es habitual.

Las entidades financieras españolas siguen sin instalar mejoras técnicas para evitar fraudes

Respecto a la seguridad técnica de las tarjetas, hay que decir que la realidad ha demostrado que la clonación de su banda magnética o la manipulación de los cajeros automáticos constituye una práctica demasiado habitual cuya razón última es que se trata de una tecnología superada. La adopción del área única de pagos (SEPA) exige que a partir del 1 de enero de 2011, el único sistema válido para tarjetas será el sistema EMV. Las entidades financieras deben incorporar a sus terminales y tarjetas de crédito y débito el llamado "chip de seguridad", un sistema que impide tanto la falsificación como la duplicidad y que sustituirá a la banda magnética, más vulnerable frente al ataque de los delincuentes. Sin embargo, a fecha de hoy sus tarjetas carecen del "chip de seguridad" ya que las entidades prefieren asumir los costes de los fraudes producidos con el dinero de plástico que adoptar el chip más seguro.

Todo ello tiene repercusiones en el ámbito jurídico. Como tendremos ocasión de ver en páginas posteriores, el problema mayor en el uso de tarjetas se da en el ámbito de la responsabilidad por su uso fraudulento. La normativa existente hasta ahora es precaria ya que son normas voluntarias desde 1988 que banco y cajas de ahorros han incorporado a los contratos de tarjeta con muchas limitaciones para los derechos de los consumidores, ha quienes hacen responder en la mayoría de las ocasiones de los robos y sustracciones de tarjeta y posterior uso fraudulento, sin probarlo ni aplicar el límite de responsabilidad de 150 euros. La futura Ley de Servicios de Pago que está en tramitación prevé, según exige la Directiva de 2007/64 sobre sistemas de pago en el mercado in-

terior, que las garantías de protección al consumidor en el uso fraudulento de tarjetas, así como el límite de responsabilidad sean de obligado cumplimiento.

2. La transferencia bancaria, un medio tradicional pero cuyo coste no está regulado

Mediante una transferencia una persona (el ordenante) da instrucciones a su entidad bancaria para que con cargo a una cuenta suya envíe una determinada cantidad de dinero a la cuenta de otra persona (el beneficiario) en la misma o en otra entidad. También pueden calificarse como transferencias aquellas operaciones en las que la orden de envío especifica que los fondos se entreguen en efectivo al beneficiario. O aquéllas en las que el ordenante paga en efectivo en la ventanilla de la entidad para su posterior envío a la cuenta del destinatario en otra entidad de crédito. En ningún caso podemos hablar de transferencia cuando lo que se realiza es la aceptación de ingresos en efectivo para su abono en una cuenta abierta en la propia entidad receptora. El ordenante de una transferencia puede hacerlo personalmente en la entidad bancaria, a través de un cajero automático, por teléfono o internet.

¿Qué tipos de transferencia pueden realizarse?

Dependiendo del ámbito geográfico existen transferencias *nacionales* si tanto el emisor como el receptor se encuentran en España, en este caso se prevé un tratamiento diferenciado cuando la transferencia supera los 12500 euros y alguno de los intervinientes sea no residente. Cuando uno de los sujetos

Los consumidores hartos de bancos y cajas por los fraudes con tarjeta



ADICAE recibió casi un 80% más de reclamaciones por fraude durante 2004. Bancos y cajas se desentienden de sus clientes y se niegan a introducir mayor seguridad.

CONSIGA TODAS ESTAS
INTERESANTES Y
AMENAS
PUBLICACIONES

Llámenos: ADICAE
C./ Gavín, 12 local. 50001 ZARAGOZA
Tfno.: 976 390060 ■ Fax: 976 390199
email aicar.adicae@adicae.net

que intervienen en la operación (ordenante o beneficiario) lo haga fuera de España, estamos ante transferencias *transfronterizas*. En este último supuesto pueden distinguirse dos categorías de transferencias, las llamadas transferencias STP (Straight Trough Processing) que son las que pueden realizarse de forma totalmente automatizada ya que la entidad posee tanto el código IBAN (número internacional de cuenta) del beneficiario y el BIC (código de identificación bancaria). Si no es así, la transferencia se llama no STP, y supone que la entidad normalmente tendrá previstas comisiones adicionales o más altas que las de una transferencia STP.

Transferencias a crédito y a débito

Pueden distinguirse también las transferencias de crédito de las de débito. En las primeras, es el propio titular de los fondos que se transmiten quien da una orden a tal efecto a la entidad de crédito en donde los fondos se encuentran depositados, o que además dará lugar al correspondiente adeudo en una cuenta bancaria. Las de débito son aquellas en las que el propio beneficiario de la transferencia o adquirente de los fondos que constituyen su objeto quien traslada a la entidad de crédito la orden de transferir fondos a su propia cuenta.

¿En qué plazo debe ejecutarse una transferencia?

En el caso de transferencias bancarias nacionales (internas), no hay plazos fijados legalmente para la ejecución de esta operación. No obstante, para las transferencias **internas** (entre sucursales de la misma entidad) se debe tomar como fecha de valoración (a efectos del cómputo de intereses) el mismo día de su orden en la oficina de origen; y para las transferencias **externas** (entre sucursales de distintas entidades), el segundo día hábil siguiente a su orden en la oficina de origen —esta fecha debe constar en la información referente a la transferencia—. Una transferencia se entenderá aceptada y se llevará a cabo, siempre que se den los requisitos necesarios, como muy tarde el siguiente día hábil a la recepción de la orden, salvo excepciones. Como vemos conceptos demasiado amplios y ambiguos que poco garantizan la seguridad de los consumidores.

Responsabilidad por transferencias deficientes o falladas

La no realización de una transferencia dará lugar a una obligación de reembolso a favor del ordenante y a cargo de la entidad a la que éste ordenó la ejecución de aquélla. Este importe tiene un límite de 12.500 euros en caso de transferencias transfronterizas. El reembolso incluirá el importe de la transferencia, los gastos que el ordenante hubiera soportado y el interés legal. Existe obligación de realizar este reembolso en el plazo de 14 días laborables contados a partir de la fecha de solicitud de reembolso que debe efectuar el ordenante.

3. El recibo bancario y la domiciliación: pese a su uso difundido aún hay cuestiones pendientes para los usuarios

El recibo bancario es un instrumento de cobro y pago al que la ciudadanía está acostumbrada ya que es la fórmula de pago a las compañías eléctricas, telefónicas, de agua, etc. Consiste en la orden de pago, dirigida al banco en el que el consumidor es titular de una cuenta bancaria, de las deudas generadas por las personas titulares de cuentas. De este modo, al vencimiento de las deudas se realizará el cargo pertinente en la cuenta de su titular.

Con esta “domiciliación” se consigue un medio de pago muy cómodo (ahorro de tiempo y trámites), ya que permite la realización de los pagos periódicos y habituales de la economía doméstica y familiar, con cargo a una cuenta bancaria, sin necesidad de trasladarse al domicilio de cada una de las empresas u organismos que le prestan un determinado servicio y que le emiten los recibos.

Requisitos para la emisión del recibo bancario:

La emisión de un recibo contra una cuenta bancaria exige autorización firmada por su titular, de forma autógrafa y por duplicado. En una de ellas se autoriza a la empresa a emitir recibos contra la cuenta y, en la otra, se autoriza a la entidad financiera a cargar los recibos presentados hasta nueva orden. Así, las entidades de crédito que emiten los recibos disponen de una base de datos en la que reflejan los datos de sus clientes.

Así mismo, cada uno de los recibos o facturas emitidas deberá reflejar los siguientes datos sobre la entidad emisora y el concepto en que se emite el recibo:

- Datos de la entidad, nombre o razón social y Número de Identificación Fiscal.
- Concepto del recibo y, si hace referencia a la liquidación de una o varias facturas, identificación de las facturas liquidadas.
- Fecha del vencimiento del recibo.
- Datos completos de la persona deudora.
- Importe del mismo con especificación del tipo de IVA aplicado y su importe.

Una vez que la entidad dispone de todos los datos y las autorizaciones de su clientela para emitir recibos para el pago de las facturas, la emisión de los recibos se realizará de forma automática.

4. El cheque: un medio de pago habitual con el que hay que tener cuidado

Es un documento por el cual una persona (la que lo emite y firma -denominado librador-) ordena a una entidad bancaria (librado) en la que tiene dinero que pague una determinada suma a otra persona o empresa (beneficiario o tenedor). A pesar de la cada vez más frecuente utilización de transferencias o tarjetas como medio de pago, el cheque sigue siendo un instrumento habitual que permite hacer frente a pagos sin necesidad de disponer de dinero efectivo.

Tipos de cheque

La primera clasificación que podemos realizar es la que se refiere al beneficiario del cobro. Distinguiamos entre cheque al portador, en el que el beneficiario es aquel que tenga el cheque, y el cheque nominativo en el que el beneficiario es aquel cuyo nombre figura en el documento. Los cheques nominativos, a su vez, pueden contener la cláusula “a la orden” que permite el endoso o traspaso a otra persona o la cláusula “no a la orden” que impediría su transmisión.

Otra modalidad de cheque es el cheque cruzado que sólo puede cobrarse a través de una entidad bancaria para que ésta a su vez lo cobre, con esto quieren reducirse los riesgos en caso de robo o pérdida. El cheque “para abonar en cuenta” sólo permitiría cobrarse mediante el abono en una cuenta bancaria.

Cheque para abonar en cuenta. Sólo se puede cobrar mediante el abono en una cuenta bancaria. O sea: no se puede cobrar en efectivo. Incluye la expresión “abonar en cuenta”.

Cheque conformado. Es aquel en el que la entidad bancaria que ha de pagarlo asegura al que lo va a cobrar que el que expide el cheque tiene fondos y que en consecuencia se pagará. Para ello, la entidad anota en el documento la expresión “conforme”, “certificado” u otra parecida y la firma. Para garantizar la operación, la entidad retiene al que expide el cheque la cantidad necesaria para pagarlo, además de la comisión que corresponda.

Cheque de viajero: Son cheques en euros o moneda extranjera emitidos por entidades bancarias u otros intermediarios financieros no bancarios de reconocida presencia internacional, como son Visa, Mastercard o American Express.

¿Cómo puede cobrarse un cheque?

Si usted es el beneficiario o poseedor de un cheque emitido por otra persona, debe tener en cuenta el plazo para el cobro que establece la Ley Cambiaria y del Cheque, 15 días desde su fecha de emisión para los

emitidos o pagaderos en España.

Existen dos posibilidades para cobrar un cheque:

Cobrarlo en efectivo en la sucursal del banco del que firma el cheque, debe tenerse en cuenta que en una sucursal distinta no habría obligación de pagar en efectivo por razones de seguridad; además podrían cobrar una comisión por razones de comprobación de validez.

Ingresarlo en su propia entidad para que se pague en su cuenta. Su entidad se encargará de cobrarle el cheque en la otra entidad en la que están depositados los fondos del que firma el cheque. Pregunte por la comisión que esta entidad va a cobrarle.

Si su entidad lo toma en firme, y se lo abona con la cláusula “salvo buen fin”, su importe se lo abonará en cuenta en la fecha en la que efectúe el ingreso y se le aplicará como fecha-valor, como máximo, el segundo día hábil siguiente a la entrega si es pagadero en otra entidad o el mismo día de la entrega si es pagadero en la misma entidad.

Llegado el momento, el cheque podría no pagarse si no existen fondos disponibles suficientes en la cuenta del librador o si hay fundadas sospechas de falsificación de su firma o se ha denunciado su robo o pérdida.

Si un cheque que ha sido presentado al cobro en el plazo legal no se paga -en todo o en parte-, tenga en cuenta que la responsabilidad es del que lo firma (el librador) y, cuando los haya, de los endosantes (los que transmitieron el documento) y de los avalistas (los que garantizan su cobro). Es a ellos a los que hay que reclamar, ya que la entidad se exime de toda responsabilidad.

La entidad bancaria librada tiene la obligación legal de pagar el cheque presentado en plazo si hay fondos disponibles suficientes en la cuenta del librador.

¿Qué hay que hacer si un cheque no se paga?

Llegado el momento, el cheque podría no pagarse si no existen fondos disponibles suficientes en la cuenta del librador o si hay fundadas sospechas de falsificación de su firma o se ha denunciado su robo o pérdida. Si un cheque que ha sido presentado al cobro en el plazo legal no se paga -en todo o en parte-, tenga en cuenta que la responsabilidad es del que lo firma (el librador) y, cuando los haya, de los endosantes (los que transmitieron el cheque) y de los avalistas (los que garantizan su cobro). Es a ellos a los que hay que reclamar. La entidad bancaria librada tiene la obligación legal de pagar el cheque presentado en plazo si hay fondos disponibles suficientes en la cuenta del librador. Si se ha presentado al cobro un cheque y la cuenta librada no tiene fondos suficientes, la entidad bancaria deberá proceder al pago parcial del mismo devolviéndolo por el importe restante y el tenedor no podrá rechazar este pago parcial.

El tomador/ tenedor del cheque tiene la capacidad de actuar judicialmente contra el librador en el momento en que se produzca el impago, debiendo aportar tan solo la documentación acreditativa de que se ha producido el impago.

5. El dinero electrónico, el futuro de los medios de pago

El dinero digital representa la generación más avanzada de los medios de pago y su futuro más prometedor. Dada la falta de precisión que existe sobre la materia, parece aconsejable comenzar delimitando el concepto de dinero digital para evitar posibles confusiones. Por ejemplo convendría establecer la diferenciación entre dinero digital y dinero electrónico. Mientras el dinero electrónico es aquel que ha sido creado, gastado y cambiado de forma electrónica, el dinero digital sólo es una clase de dinero electrónico que se identifica con la asignación de un valor económico a una serie de dígitos.

De qué hablamos cuando hablamos de dinero electrónico

El “dinero electrónico” es un valor monetario representado por un crédito exigible al emisor:

- a) Almacenado en un soporte electrónico.
- b) Emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido.
- c) Aceptado como medio de pago por empresas distintas del emisor. Este concepto es más amplio que el de dinero digital y en él se engloban modalidades como “Netcheque” (posibilidad de emitir cheques digitales), “Cibercash” (posibilidad de realizar pagos en Internet a partir de una tarjeta de crédito), el propio dinero que tenemos en un monedero electrónico, o el pago realizado por medio de tarjetas. El portador de dinero electrónico podrá, durante el período de validez, solicitar al emisor que se lo reembolse al valor nominal por monedas y billetes de banco o por transferencia a una cuenta, sin otros gastos que aquellos que resulten estrictamente necesarios para realizar la operación. El contrato entre el emisor y el portador estipulará claramente las condiciones de reembolso, pudiendo prever un límite mínimo para el mismo, que no podrá superar los diez euros.

En los supuestos de dinero digital, la entidad que lo emite crea “billetes digitales” por la cantidad que el cliente requiera, estando formado cada “billete” por una secuencia de 15 dígitos que opera en Internet mediante un software específico para él. Una vez creados los billetes digitales, el particular solo podrá

utilizarlos desde su ordenador personal si tiene ese software especial y posee el hardware necesario para hacerlo. El hardware del ordenador personal consiste en una tarjeta inteligente (al igual que tiene una tarjeta de red o una tarjeta de televisión) llamada “wallet”, que será en la que se almacene el dinero digital. Las características que se le viene exigiendo a este dinero digital son: seguridad, anonimato, que sea transportable, transferible, divisible, de duración indefinida y generalmente aceptado.

Un medio aún más reciente: Pago desde el teléfono móvil

El pago por móvil es un servicio que permite realizar pagos y otras transacciones bancarias en cualquier momento y lugar. Pagar desde el teléfono móvil constituye la última posibilidad que se le está ofreciendo a los consumidores de llevar a término un pago electrónico.

Este nuevo servicio se dirige especialmente a los pagos de escasa cuantía, entradas de cine, taxis, etc. La ejecución de una operación de pago electrónico desde el teléfono móvil varía según el operador, pero en todos ellos aparece una entidad de crédito autorizando o negando la operación. La operativa consiste en asociar a un teléfono móvil una o varias tarjetas electrónicas emitidas por una entidad financiera.

A día de hoy, la propia tarjeta SIM (Módulos de Identidad del Abonado) hace las veces de tarjeta de crédito. Existe una “clave de autorización personal” similar al PIN de las tarjetas para cada medio de pago, que es gestionada por la entidad emisora, la cual sólo es conocida por el titular. El usuario autoriza cada transacción mediante la introducción del PIN, siendo equivalente al consentimiento de una firma.

El “Fraude”, un delito contra los intereses económicos de los usuarios

La expresión “fraude en medios de pago” designa de manera genérica un conjunto de actuaciones de muy diversa naturaleza que hacen referencia a la comisión de una serie de ilícitos que afectan a los derechos de los consumidores en cuanto usuarios de medios de pago.

En particular, en el ámbito del derecho, el término “fraude” hace referencia a una pluralidad de actuaciones y tipos contrarios a la legalidad que tienen características y consecuencia jurídica distintas. No es lo mismo el “fraude a la ley” que recoge el artículo 6.4 del Código Civil (y como ejemplo de aplicación concreta, el “fraude de ley tributaria”, un conflicto de aplicación de la norma tributaria que lleva a aplicar la correspondiente norma que se ha pretendido eludir), que el “fraude” que recoge el artículo 436 del Código Penal, como infracción del deber de lealtad que un funcionario debe guardar en la gestión de un servicio público, y que lleva aparejada la aplicación de una pena; o el “fraude procesal” del artículo 11.2 de la Ley Orgánica del Poder Judicial.

Por tanto creemos que, a los efectos de este Estudio, definir con precisión qué entendemos por “fraude” cuando hablamos de “fraude en medios de pago”, constituye una tarea previa necesaria. En este sentido, es evidente que dados los medios y las consecuencias derivadas de las actuaciones en este ámbito, hablar de “fraude” en los

sistemas de pagos significa la comisión de un delito de estafa, en cuanto engaño con intención de obtener un lucro. Esto lo veremos con detenimiento en las líneas siguientes.

Una vez planteado todo esto, a continuación vamos a analizar con detalle, qué se entiende, desde la perspectiva penal por “fraude en medios de pago”, con especial referencia al uso de tarjetas, como elemento de pago más común y extendido y, por tanto, más problemático.

¿Qué entendemos por fraude?

La Real Academia de la Lengua Española define el concepto de fraude como la “acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete”. Por tanto, los elementos fundamentales para poder designar como fraude a una acción es que sea contradictoria a la verdad, por lo tanto engañosa, y que suponga un perjuicio contra quien se comete.

Las entidades de crédito también defraudan las expectativas de los consumidores

No obstante, aún cabe hacer mención a una acepción más en este ámbito que, la mayor parte de las ocasiones no se toma en cuenta. Es la noción de “fraude” en cuanto “fraude a las expectativas de los consumidores en cuanto al uso del medio de pago contratado y sus consecuencias”. En efecto, cuando un consumidor contrata la utilización de uno de estos medios de pago (pensemos en una tarjeta), o hace uso de ellos (una transferencia), espera que razonablemente el servicio se cumpla, la función de la tarjeta o la transferencia se lleve a cabo tal y como estaba previsto, y, finalmente, que los sistemas de seguridad de las mismas sean adecuados, dado que nos encontramos ante sistemas complejos que normalmente se escapan a la pericia del consumidor, y que constituye un medio a través del cual se transmite un dinero (ahorros, sueldo, etc.) propiedad del consumidor. Pues bien, en demasiadas ocasiones, ni se presta el servicio adecuadamente (una tarjeta que es rechazada por un comerciante cuando debería aceptarla); ni es justo el sistema de retribución por su uso (comisiones excesivas por la utilización de una transferencia); ni, por lo que interesa a este Estudio, el sistema funciona adecuadamente, lo que muchas veces pone en riesgo los legítimos intereses económicos de los usuarios (por ejemplo un cajero automático manipulado que debería haber sido supervisado con diligencia por la entidad de crédito).

En el ámbito jurídico, en el que nos centramos, la comisión de estas acciones pueden tener como resultado la afeción a los derechos personales (como es el caso de los datos privados) o a los derechos patrimoniales de los consumidores; estaríamos en este último supuesto ante lo que se conoce como “estafa”. No cabe duda, como tendremos ocasión de recoger en este estudio, de que los fraudes efectuados en medios de pago entran dentro de este supuesto, si bien con caracteres propios y particulares.

El delito de estafa: el ánimo de lucro como fin y el engaño como medio

La comisión de alguno de los delitos que se caracterizan por el ánimo de lucro como fin y el engaño o abuso de confianza como medio es la definición que la Real Academia de la Lengua otorga al término estafa. En el estricto ámbito jurídico, el Código Penal en su artículo 248 manifiesta que “cometen estafa los que, con ánimo de lucro, utilizan engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio y ajeno”.

La complejidad que este término presenta requiere un análisis, si quiera resumido, de los distintos elementos que lo conforman:

1) El engaño

Es el elemento que caracteriza a la estafa frente a otros delitos de contenido patrimonial. Este puede materializarse tanto a través de una acción como de una omisión, ya que también a través de la inactividad o el silencio puede cometerse engaño.

2) El error en el sujeto pasivo (consumidor)

Para hablar de estafa necesariamente el engaño debe producir un error esencial en el sujeto pasivo que por causa del engaño del autor del delito desconoce o tiene un conocimiento deformado o inexacto de la realidad. El error lleva al sujeto pasivo a actuar bajo el conocimiento inexacto o falso de la realidad y a emitir una manifestación de

voluntad viciada por la que pone su patrimonio a disposición del autor y en su beneficio.

3) Acto de disposición

El sujeto pasivo del engaño, a consecuencia de este, realiza un acto de disposición que implica un desplazamiento de su patrimonio, desplazamiento que le genera un perjuicio, a la vez que supondrá un beneficio para el autor del delito o falta. Será clasificado el hecho de delito cuando el perjuicio tenga un valor superior a 400 euros, ya que si el valor es inferior a esta cantidad será tipificado como falta, de acuerdo al artículo 623 del Código Penal.

Necesariamente el perjuicio debe ser consecuencia del engaño, en caso contrario no podríamos hablar de estafa.

4) Ánimo de lucro por el infractor

El propósito del infractor es obtener una ganancia patrimonial correlativa al perjuicio ocasionado, aunque no necesariamente tiene que ser equivalente.

Los emisores de medios de pago imponen los contratos y se eximen de responsabilidad

Sin perjuicio de las responsabilidades de terceros, sobre todo en la comisión de delitos, en muchas ocasiones las propias entidades se eximen de su responsabilidad, cuando es de su incumbencia poner a disposición del consumidor medios y herramientas de pago con la máxima seguridad y las mayores garantías en su uso. Son ellas a las que cabe exigir la mayor diligencia, por su posición de predominio que ocupan en la relación contractual, tanto técnica como jurídicamente. En este caso, otro aspecto en el que se defraudan las expectativas de los consumidores es en cargar toda la responsabilidad en el consumidor, en los casos de ataque de terceros a través del medio de pago, mediante prácticas y, sobre todo, cláusulas abusivas en los contratos que limitan la responsabilidad de las propias entidades.

¿Qué entendemos por fraude en medios de pago?

En sentido amplio, cualquier tipo de conducta tipificada como delictiva, la cual vulnera los derechos de los consumidores en su faceta de usuarios de medios de pago distintos del efectivo, entendidos como tales los definidos en el apartado anterior. En el ámbito penal se trata de una estafa con características propias y particulares.

Clases de fraude en Medios de Pago y sus consecuencias para el consumidor

Una de las notas características de los fraudes en medios de pago es su variedad. El uso de las nuevas tecnologías y de actuaciones de "ingeniería social" (prácticas cuyo objetivo es engañar los consumidores a partir del abuso de confianza y la buena fe) ha determinado que estos fraudes sean además constantemente renovados, por lo que es muy difícil establecer una clasificación cerrada.

1. El fraude y la estafa en los medios de pago

Dada la difusión y el uso cada vez más extendido de los medios de pago, estos constituyen hoy en día uno de los instrumentos más utilizados por aquellos que cometen fraudes y estafas. Si bien inicialmente las tarjetas de crédito y débito supusieron el objeto principal de los fraudes patrimoniales, la generalización del conocimiento de la informática y las nuevas tecnologías, han hecho aumentar vertiginosamente los fraudes tanto en número como en cantidades defraudadas. Y es que Internet ha permitido la comisión de estafas masivas en número hasta ahora desconocido, dejando desfasada la legislación en muchos casos y provocando que debido a la complejidad de estas y a su distinta tipológica que en la mayoría de las ocasiones las autoridades estén un paso por detrás de los estafadores.

Esta realidad hace necesario el establecimiento de sistemas de seguridad eficaces en la transmisión y cesión de datos, mejorar la información al usuario sobre posibles fallos y responsabilidades y crear una legislación adecuada que permita que los titulares de medios de pago no se hallen continuamente en una situación de indefensión e inseguridad.

Hablar hoy día de los medios de pago significa, por su progresiva introducción, hacer referencia a las nue-

vas tecnologías, en concreto a la informática y la web, así como su expresión en ámbitos financieros, el e-banking o banca por Internet.

Medios de pago y delitos informáticos

Un "delito informático" es aquel que, tipificada su conducta como tal en la ley, se cometa utilizando tecnologías de la información y comunicaciones (pensemos en el envío de un correo donde se nos pide que incluyamos nuestro número de cuenta o tarjeta). A la novedad de este tipo de delitos, se une su mayor complejidad. En efecto, las características fundamentales de estos delitos son:

- **La Transnacionalidad:** los delitos informáticos superan los límites fronterizos de los estados, por ello se exige cooperación y regulación supraestatal. Hasta ahora la solución adoptada ha sido la de perseguir el delito por la autoridades competentes del Estado en el que la víctima sufre sus consecuencias.

- **Distancia Física:** determinar la localización del delincuente es difícil por cuanto no se da simultaneidad entre el lugar del crimen y la presencia de quien lo ha cometido.

- **Ubicuidad:** las nuevas tecnologías permiten que se cometan delitos al mismo tiempo

- **Presencia de redes de delincuencia** organizada: bandas que emplean mecanismos y programas in-



Los sistemas de pago electrónico: ¿fiables y seguros?

Para que se produzca una definitiva implantación de las novedades desarrolladas en la forma de realizar nuestros pagos, se debe asumir las reivindicaciones más tradicionales de los usuarios: comodidad, operatividad y, fundamentalmente, seguridad en sus derechos.

CONSIGA TODAS ESTAS
INTERESANTES Y
AMENAS
PUBLICACIONES

Llámenos: ADICAE
C./ Gavín, 12 local. 50001 ZARAGOZA
Tfno.: 976 390060 ■ Fax: 976 390199
email aicar.adicae@adicae.net

formáticos complejos y que actúan, ya sea a través de la red, como en medios físicos (cajeros, copia de bandas magnéticas...)

Formas de cometer estos delitos:

Delitos basados en “técnicas de ingeniería social”: en los que el consumidor afectado es engañado para hacer algo que normalmente no haría, ya que supone un perjuicio económico para él. Por ejemplo, revelar las claves de su cuenta por Internet.

Delitos que aprovechan la vulnerabilidad de los sistemas. Por ejemplo el uso de bandas magnéticas en tarjetas que son fácilmente clonables. Esta forma de delitos requiere lógicamente una dotación técnica notable por parte de los delincuentes.

2. Ingeniería social y nuevas tecnologías al servicio del fraude

Podemos establecer una clasificación de actuaciones fraudulentas, de conformidad a la Decisión Marco del Consejo 2001/413/JAI, de 28 de mayo de 2005:

- El robo o la apropiación indebida de instrumentos de pago;
- La falsificación o la manipulación de instrumentos de pago, para su utilización fraudulenta;
- La recepción, la obtención, el transporte, la venta o la transferencia a un tercero, o la posesión y el uso fraudulento de instrumentos de pago sustraídos, falsos o alterados;
- La introducción, modificación y eliminación no autorizada de datos electrónicos o la interferencia no autorizada en el funcionamiento del programa o del sistema electrónico, y
- La producción, recepción, venta o creación fraudulenta de instrumentos, programas u otros medios adaptados específicamente para llevar a cabo las acciones anteriormente mencionadas.

Todas estas actuaciones son tipos genéricos que engloban una pluralidad de actuaciones concretas que conviene conocer y evaluar.

3. Delitos que aprovechan la vulnerabilidad de los sistemas

■ El “skimming”: copiar digitalmente la información de la tarjeta

El “skimming” consiste en obtener los datos de la tarjeta de un usuario y acceder al dinero de su cuenta asociada.

Puede ocurrir cuando un cliente paga con tarjeta en un comercio y un empleado desleal copia la información de la banca magnética con un lector. Estos lectores son de tamaño mínimo, los hay de dimensiones similares a una pinza, por lo que a veces es difícil darse cuenta. La información es transferida a otras tarjetas en blanco mediante programas informáticos y quedan listas para ser utilizadas en establecimientos, aunque no para reintegros, al no conocerse el número secreto del estafado.

Los estafadores elaboran incluso documentos para respaldar las nuevas tarjetas, de forma que a nombre de una sola persona pueden funcionar hasta ocho o diez tarjetas falsas.

Una variante de este fraude se produce cuando los estafadores colocan lectores en la entrada de los cajeros de tarjetas. Camuflan además una minicámara sobre el teclado que envía la información por medio de un transmisor de radio hasta un punto cercano donde los timadores descifran la información.

■ La “siembra”: despistar a la víctima y dar el “cambiao” a la tarjeta

Asimismo, existe una segunda modalidad conocida como “la siembra”, que tiene por objeto conseguir el número PIN y de la tarjeta de crédito de la víctima. Una persona se sitúa a una distancia adecuada de quien se encuentra efectuando una operación en un cajero e intenta ver su número PIN. A continuación, trata de distraerle para que pierda de vista la tarjeta cuando sale por la ranura del cajero.

Las tarjetas obtenidas por este procedimiento son utilizadas para extraer dinero de los cajeros y, cuando dejan de ser válidas por alcanzar el límite de disposición en efectivo prefijado, son utilizadas como soporte para fabricar otras tarjetas y realizar nuevas operaciones con éstas.

■ “Phishing”: “pescar” información privada de usuarios incautos de la red

Consiste en robarle la identidad al usuario de páginas Web dedicadas bien a la compra online o páginas de banca electrónica. El delito comienza cuando los estafadores obtienen información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos por medio del correo electrónico o de ventanas emergentes. Parecen provenir de sitios Web reconocidos o de confianza para la víctima, como su banco, la empresa de su tarjeta de crédito o su tienda habitual de compra online, y es ahí donde reside su peligrosidad.

Dado que estos mensajes y sitios Web parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos.

■ **“Pharming”:** acceder a un ordenador ajeno mediante software

Lo particular de este tipo de estafa es que se produce sobre ordenadores que están infectados por un troyano (un tipo de software malicioso); que permite a otros usuarios entrar al ordenador de otro usuario.

Los estafadores acceden al ordenador de la víctima y manipulan el código de resolución de nombres en internet. Cuando el usuario estafado accede a la página de su banco o a una de compras online, en realidad está entrando a la IP de una página Web falsa, de forma de cuando escribe sus claves estas son capturadas por el estafador.

■ **“Smishing”:** fraude mediante el teléfono móvil a costa del destinatario

Funciona a través del envío de mensajes SMS de telefonía móvil. Se produce mediante una suplantación de identidad, que permite a los estafadores acceder a datos fundamentales de los que se sirven para obtener un beneficio monetario a costa del destinatario de los mensajes.

■ **“Escrow”:** hacerse pasar falsamente por una empresa consignataria

También conocido como “depósitos en garantía”, el denominado “Escrow” es un método de fraude que ha surgido a raíz de las operaciones de venta en Internet. Los estafadores se aprovechan de la creación de empresas consignatarias legales, que se dedican a custodiar el bien adquirido por el consumidor hasta que éste lo recibe en su casa y muestra su conformidad; todo ello a cambio de realizar un pago como garantía.

El engaño consiste en simular ser una compañía consignataria y obtener el dinero del comprador online como si fuera realmente una de estas empresas. El fraude es doble porque, además, los estafadores obtienen datos de la víctima para engañarla en sucesivas ocasiones.

Consecuencias jurídicas de los fraudes en medios de pago para el consumidor

La relación expuesta de los fraudes en medio de pago tienen todas en general una serie de consecuencias concretas para los consumidores afectados. Este tipo de delitos afectan a los derechos de intimidad y privacidad garantizados por nuestra constitución y tutelados por distintas leyes, y en ocasiones afectan al funcionamiento de una herramienta del consumidor, como es el sistema operativo que queda inutilizado o no responde con un funcionamiento adecuado. Pero sobre todo, y de manera especialmente intensa, afectan a los derechos económicos de los usuarios (salarios, pensiones, ahorros...)

En todos estos tipos de fraude descritos tiene lugar, de manera destacada, una transferencia no consentida, una disposición patrimonial, sin consentimiento del titular y por tanto lesivo para su legítimos intereses.

Parte 2

Retos y deficiencias de la normativa europea en la protección del consumidor ante el fraude en medios de pago



A la hora de trazar el panorama normativo que regula los medios de pago y su control para evitar los fraudes a los usuarios, es necesario advertir que los medios de pago tienen su origen en relaciones privadas entre particulares. A diferencia del dinero, cuyo origen privado derivó en un control público notable y amplio de tal forma que son instituciones públicas quienes lo emiten, esta circunstancia todavía no se da en el ámbito de los medios de pago distintos del dinero en efectivo. Son las grandes empresas y corporaciones las que ponen en el mercado una serie de instrumentos técnicos cuya finalidad es facilitar las transacciones comerciales.

En el mismo sentido los contratos que regulan el uso y disposición de estos medios de pago son también elaborados unilateralmente por las empresas y el consumidor no puede intervenir en su confección. Como consecuencia, el derecho que nace es un derecho "contractual": nace de los contratos privados y posteriormente se incorpora a los derechos nacionales- transnacionales. Y es aquí donde la protección al consumidor, como derecho de naturaleza público-privada pero también como principio transversal que obliga a los Estados modernos y, en concreto a la Unión Europea, debe jugar un papel importante.

A continuación trazaremos un recorrido por los convenios, normas, decisiones y recomendaciones que, ha nivel Europeo y Estatal, se han dirigido a proteger a los usuarios de los ataques de terceros que se han aprovechando la fragilidad de los sistemas puestos en el mercado como instrumentos de pago. Posteriormente nos centraremos en la protección que ofrece el derecho penal español en los supuestos de estafas en medios de pago.

Por último añadir que en los Anexos a este Estudio, recogemos una amplio catálogo normativo (protección civil y penal) de la distinta normativa de los países participantes en el proyecto Europeo encabezado por ADICAE, sobre la protección de los derechos de los consumidores en los fraudes con tarjetas.

Medidas contra el fraude en la Unión Europea: control de contratos, fijación de responsabilidades y prevención

La UE ha mostrado su preocupación por adoptar medidas, al menos desde 1997, para evitar los hechos ilícitos de los medios de pago distintos del efectivo. Las perspectivas de la UE son las de aseguramiento y fomento de la actividad económica, la de protección del consumidor, y en alguna medida, la de la lucha contra la criminalidad organizada y no la estrictamente penal, pero a través de ciertas medidas comunitarias con incidencia en las legislaciones penales internas propone la incriminación de conductas y otras medidas tendentes a la protección de este tipo de medios de pago. Pese a todo, la lentitud de los acuerdos, muchos de ellos meras declaraciones de intenciones de carácter programático cuando no testimonial, está afectando al desarrollo y potenciación de una economía basada en las nuevas tecnologías, la extensión de un mercado europeo seguro y sobre todo, está generando desconfianza entre los consumidores y usuarios, pieza clave para cumplir con lo subjetivos anteriores.

1. Los códigos y las “buenas prácticas” no son suficientes para proteger a los consumidores

(Recomendaciones de la Comisión Europea 87/598 y 88/590)

La primera de las referencias de la normativa europea a la hora de tratar el tema de los medios de pago en su vertiente jurídico-privada (derechos y obligaciones entre emisores de tarjeta-- bancos y cajas-- y consumidores) se estableció a través de dos recomendaciones a finales de los años ochenta.

El problema no resuelto de la responsabilidad

La Recomendación de la Comisión Europea 87/598 de 1987 sobre el Código de Buena Conducta en materia de pago electrónico, estableció una serie de principios generales de comportamiento a través de un Código de “Buena Conducta” cuyo propósito era alcanzar la compatibilidad y complementariedad entre los distintos sistemas de pago. A través de este Código se dejaba, en definitiva, que fuesen las propias entidades financieras para que decidieran acerca de la compatibilidad de ellos diferentes sistemas.

Posteriormente se dictó la **Recomendación 88/590** sobre las relaciones entre titulares y emisores de tarjetas donde se estableció la **responsabilidad por el uso fraudulento en caso de pérdida o robo de una tarjeta hasta la notificación del hecho al emisor que se fijó en el límite de 150 euros, exceptuando los casos en que se haya actuado de forma fraudulenta o negligentemente grave** (en cuyo caso no se aplicará este límite). Esta Recomendación fue modificada por la Recomendación 97/489, por lo que analizaremos su contenido de modo más amplio al tratar esta Recomendación.

El banco debe impedir el mal uso

No obstante, **el responsable de impedir el mal uso de la tarjeta es el emisor (Banco o Caja) que debe responder por las circunstancias relativas al funcionamiento del sistema** ya que es quien conoce o debería conocer los riesgos y limitaciones de este. Por este motivo, es el emisor quien tiene la carga de la prueba, en su caso, respecto a la posible negligencia o mala fe del usuario de la tarjeta, y nunca trasladarla directamente al consumidor, como lo hacen a través de ellos contratos de adhesión muchas entidades financieras.

Hay que recordar que la relación jurídica que se establece entre el emisor y el usuario de la tarjeta de crédito se instrumenta a través de un contrato de tarjeta de crédito, contrato que es de adhesión ya que las cláusulas son impuestas unilateralmente por la entidad emisora limitándose el consumidor a firmarlo. La complejidad junto con la falta de regulación hacen que, en el momento actual, **ningún sistema pueda garantizar una seguridad completa ya que la normativa en su conjunto no sólo es dispersa sino que a todos los efectos resulta insuficiente**. No obstante, la Directiva 2007/64, como veremos más adelante, establece obligatoriedad legal a estos límites de responsabilidad de 150 euros, superando por fin la voluntariedad que imperaba en este ámbito.

2. Las “normas blandas” no son la solución para los consumidores

(Recomendación de la Comisión de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago)

El objetivo de esta Recomendación es establecer un marco común en el territorio de la Unión Europea en relación a los elementos esenciales de las relaciones entre emisores de instrumentos electrónicos de pago

(bancos y cajas de ahorros) y titulares de los mismos (los consumidores y usuarios), incluyendo la información mínima que deberá facilitarse al cliente en relación a las transacciones efectuadas mediante aquéllos. Esta Recomendación completa y sustituye a la Recomendación de 1988/590, relativa a “sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjetas”.

La Recomendación “invita” al cumplimiento de ciertas previsiones, a destacar:

- *El contrato relativo a la tarjeta, que deberá formalizarse por escrito -o, en su caso, por medios electrónicos- deberá contener, de forma clara y comprensible, todas las condiciones aplicables al mismo, que se referirán, entre otros, a la descripción del conjunto de derechos y responsabilidades del titular y del emisor así como a las condiciones económicas (cuota periódica, comisiones bancarias, etc.).*
- *El emisor deberá facilitar al titular información sobre las transacciones efectuadas que permita su adecuada identificación*

Se declara la obligación del titular de preservar el dato de su número de identificación personal.

Normas blandas e inseguridad jurídica

Sin embargo, **esta recomendación de 1997** (al igual que la anterior de 1988 ya comentada) **no tiene carácter de norma vinculante para las entidades financieras, por lo que la utilidad de las previsiones en ella contenida se ha demostrado insuficiente para garantizar una defensa eficaz de los derechos de los consumidores** frente a los fraudes en medios de pago. Se incumple así, incluso, las exigencias de la normativa de la UE de garantizar un alto nivel de protección a los consumidores. Buena parte del contenido de la Recomendación ha sido incorporado voluntariamente por parte de los emisores en los contratos relativos al uso de instrumentos electrónicos que suscriben con su clientela, con las consecuencias negativas de inseguridad para los usuarios como veremos más adelante.

El límite de 150 euros se incumple reiteradamente

El titular sólo asumirá los daños derivados de la pérdida o robo del instrumento hasta que notifique al emisor tales circunstancias, y en este caso hasta un determinado límite, que no excederá de 150 euros. En cualquier caso **el titular no será responsable si el instrumento de pago se utilizó sin presentación física o identificación por medios electrónicos del instrumento mismo.**

El emisor sólo podrá modificar las condiciones del contrato cuando lo notifique personalmente y con antelación suficiente al titular. Si en el plazo de un mes el ti-

tular no hubiera denunciado las nuevas condiciones, se entenderán aceptadas.

El emisor se compromete, entre otros, a preservar el número de identificación; a no enviar instrumentos no solicitados -salvo que se trate de una reposición, a mantener un registro interno de las transacciones realizadas así como a poner los medios adecuados para permitir al titular la notificación de incidencias en cualquier momento del día o de la noche.

El emisor se responsabiliza de la no ejecución o ejecución defectuosa de las transacciones del titular, de las transacciones no autorizadas por éste o de cualquier error atribuible al emisor en relación con la gestión de la cuenta del titular, asumiendo las consecuencias financieras derivadas de éstos.

3. Protección para las transferencias intracomunitarias que no se aplicó a la operativa interna (Directiva 97/5/CE)

La Directiva 97/5/CE, del Parlamento Europeo y del Consejo, de 27 de enero de 1997, relativa a las transferencias transfronterizas, tuvo como objetivo que estas transferencias se realicen de una manera rápida, fiable y económica, dentro del espacio único europeo. Para ello se establecía una serie de obligaciones mínimas de las entidades que realicen transferencias entre Estados miembros de la Unión Europea así como las consecuencias jurídicas del incumplimiento de tales obligaciones, y ello al margen de la responsabilidad común de las entidades respecto del quebrantamiento de normas de derecho privado cuyo conocimiento corresponderá a la jurisdicción ordinaria.

Un uso mayor de las transferencias transferencias

La Directiva 97/5/CE reguló, hasta su derogación por la Directiva 2007/64 como veremos en el punto siguiente, las transferencias realizadas entre entidades situadas en distintos Estados miembros de la Unión Europea. Las transferencias reguladas por la Directiva son transferencias de crédito (es decir, dadas por el ordenante titular de la cuenta de cargo) tienen un importe limitado (50.000 euros), realizadas en una moneda determinada (euros o divisas de los Estado miembros) y respecto de las que se prevé, especialmente, la intervención de particulares y pequeñas y medianas empresas (Considerando Segundo Directiva 97/5/CE), excluyéndose, de forma expresa, las transferencias ordenadas por sujetos profesionales del mercado financiero (art. 1 Directiva 97/5/CE) En este sentido, **esta Directiva revela un cierto carácter proteccionista respecto a los usuarios de los servicios financieros.**

Celeridad, fiabilidad y seguridad en las transferencias

Esta Directiva, imponía a las entidades que intervienen en la realización de transferencias entre Estados miembros de la Unión Europea una serie de obligaciones para garantizar a los usuarios unos mínimos de celeridad y fiabilidad de la operación. Esas obligaciones se refieren, básicamente al cumplimiento de los plazos voluntaria o legalmente estipulados y al seguimiento de las instrucciones recibidas del ordenante, fundamentalmente en lo relativo al cargo de los gastos que implique la transferencia. También contemplaba la obligación concreta de indemnizar al ordenante por retraso en la acreditación de los fondos en la cuenta de la entidad del beneficiario y de la de resarcir al beneficiario por retraso en practicar el abono correspondiente en su cuenta,

Conforme a esta Directiva, la entidad del ordenante debía realizar la transferencia en el plazo que acordado con éste. Para el caso de que no se hubiese convenido un plazo, **se conceden a la entidad cinco días laborales bancarios, contados desde el día siguiente a la fecha de aceptación de la orden de transferencia, para acreditar los fondos en la cuenta de la entidad del beneficiario.** Por fecha de aceptación se entendía aquella

en la que se reúnen todas las condiciones necesarias para poder ejecutar la orden es decir, la fecha en la que se han proporcionado todos los datos exigidos por la entidad y en la que existe cobertura financiera suficiente.

Si la entidad no cumple con el usuario debe indemnizarle

Salvo que la entidad pueda demostrar que ha solicitado al cliente información o condiciones adicionales se presumirá que esas circunstancias se dan, como muy tarde al día hábil siguiente de haber sido impartida la orden. A partir de entonces la entidad del ordenante cuenta con cinco días —durante los cuales quizá deba producirse la intervención de entidades intermediarias— para que los fondos lleguen a ser acreditados en la entidad del beneficiario. **En el supuesto de cumplimiento tardío de esta obligación, por no haberse respetado los plazos mencionados el ordenante, debía ser indemnizado por su entidad** —aunque no sea la responsable directa del retraso. La cantidad a abonar como indemnización será el interés legal del dinero multiplicado por 1,25 (así lo recoge la ley 1/1999 que transpuso esta Directiva 97/5 al ordenamiento jurídico español) calculado sobre el importe de la transferencia y

LOS PRINCIPIOS PARA UN MERCADO INTERIOR DE PAGOS OLVIDAN LA SEGURIDAD

(Comunicación de la Comisión Europea de 31 de enero de 2000)

En esta Comunicación, la Comisión puso de manifiesto los principios para crear una zona única de pagos. No obstante olvidó vincularla a la importante cuestión de la seguridad a la hora de realizar estas transacciones.

- 1. Mejorar la eficiencia y la relación coste-eficacia de los pagos, en particular las transferencias.*
- 2. Mejorar la infraestructura básica de las transferencias puede ser también fundamental para mejorar otras operaciones como pagos directos y otras transferencias entre cuentas.*
- 3. Las comisiones percibidas por transferencias transfronterizas deberán reducirse sustancialmente hasta los niveles nacionales corrientes.*
- 4. En la medida de lo posible, los plazos de los pagos transfronterizos no superarán en más de un día los plazos de pagos nacionales. La duración total de un pago transfronterizo no deberá exceder en más de un día el tiempo que requiere un pago nacional. Con esto se trataba de superar el excesivo plazo otorgado en la Directiva 97/5 sobre Transferencias en el Mercado Interior.*
- 5. Las comisiones por una transferencia transfronteriza en principio deberán ser soportadas en su totalidad por el ordenante y no cobrarse al beneficiario de acuerdo con las prácticas nacionales en la mayoría de Estados de la UE. Posteriormente, como tendremos ocasión de comprobar cuando analicemos la Directiva 2007/64 de Servicios de Pago en el Mercado Interior, el sistema ha cambiado ya que se pasa a un sistema por el que los proveedores de servicios de pago (bancos, cajas, etc.) pueden cobrar al ordenante y al beneficiario de la orden de pago. Aquí puede apreciarse la influencia del lobby bancario.*
- 6. Evitar la proliferación de normas. Las normas existentes se aplicarán lo antes posible. La cuestión de la autorregulación seguían siendo importante, pese a los problemas que normas como las Recomendaciones de 1988 y 1997 han resultado ser muy perjudiciales para los derechos de los consumidores.*
- 7. Los sistemas de pago transfronterizos debían ser accesibles.*

aplicado al período de tiempo transcurrido entre el término del plazo convenido o, en su defecto, el legalmente señalado para la acreditación de los fondos en la cuenta de la entidad del beneficiario y la fecha en que efectivamente se produzca dicha acreditación.

La entidad del beneficiario tiene también obligación de poner a disposición de su cliente los fondos resultantes de la transferencia dentro del plazo que hubiera convenido con él. Para el caso de que no se haya acordado plazo, se prevé igualmente una regla supletoria. **La puesta a disposición deberá realizarse, a más tardar, el día laborable bancario siguiente a la acreditación de los fondos en la cuenta de la entidad. El retraso en el cumplimiento de esta obligación trae consigo para ella el deber de indemnizar a su cliente.** La indemnización consistirá en el abono del interés legal del dinero multiplicado por 1,25 calculado sobre el importe de la transferencia y aplicado al período transcurrido entre el término del plazo convenido para la puesta a disposición de los fondos o, en su defecto, el legalmente señalado y la fecha en que efectivamente se realice el abono en la cuenta del beneficiario. También en este caso se señala el carácter no excluyente de esta indemnización respecto a la que, por daños y perjuicios, pudiera reclamar el cliente a su entidad o respecto a los derechos que pudieran corresponder a ésta.

4. Una buena regulación del uso fraudulento de tarjeta en las ventas a distancia (Directiva 97/7)

La Directiva 97/7/CE en materia de contratos a distancia regula todo contrato entre un proveedor y un consumidor sobre bienes o servicios, celebrado en el marco de un sistema de ventas o de prestación de servicios a distancia organizado por el proveedor en el que se utilice exclusivamente una o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato. Esta Directiva entiende por “técnica de comunicación a distancia”: todo medio que permita la celebración del contrato entre un consumidor y un proveedor sin presencia física simultánea del proveedor y del consumidor.

Esta Directiva resulta importante en el ámbito de los medios de pago puesto que en su artículo 8 se previene contra el fraude en tarjetas en las compras a distancia. Este artículo dice que **“Los Estados miembros velarán por que existan medidas apropiadas para que:**

- **el consumidor pueda solicitar la anulación de un pago en caso de utilización fraudulenta de su tarjeta** de pago en el marco de contratos a distancia cubiertos por la presente Directiva;
- **en caso de utilización fraudulenta, se abonen en cuenta al consumidor las sumas abonadas en concepto de pago o se le restituyan”.**

Esta Directiva, y su artículo 8 se incorporaron al ordenamiento jurídico español a través de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (modificada posteriormente por la Ley 47/2002, de 19 de diciembre). En su artículo 46 se dio cumplimiento a esta Directiva incluyendo un artículo 46 (que posteriormente se incluyó como artículo 106 en la Ley General de Consumidores y Usuarios, Real Decreto Legislativo 1/2007).

El consumidor puede reclamar el cargo de una compra fraudulenta por internet pagada con tarjeta

1. *Cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, el consumidor y usuario titular de ella podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad.*
2. *Sin embargo, si la compra hubiese sido efectivamente realizada por el consumidor y usuario titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución, aquél quedará obligado frente al empresario al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación.”*

5. Grupo de expertos en la materia de cara a la ampliación de la Union (Plan de Acción de la UE (2004-2007) para la prevención del fraude de los medios de pago distintos del efectivo)

En el avance de los trabajos de la Comisión sobre los medios de pago distintos del efectivo se realiza una Comunicación al Consejo, al Parlamento europeo, al Comité Económico y Social, al BCE, y a Europol con un nuevo plan de acción de la UE (2004-2007) para la prevención del fraude de los medios de pago distintos del efectivo. En la misma se señala, con notables muestras de conformismo, que las medidas previstas por el plan de acción 2001-2003 para la prevención del fraude (PAPF) habían sido un éxito. Con el fin de garantizar un eficaz intercambio de información a nivel europeo, **la Comisión considera necesaria en el ámbito de la prevención del fraude una clarificación de la legislación comunitaria y nacional en materia de protección de datos.**

En la mencionada Comunicación se fija por parte de la Comisión las prioridades para mantener y mejorar la cooperación entre todos los actores, que se detallan de forma particularizada:

Hay que mejorar la formación de las autoridades competentes en materia de represión del fraude. La Comisión tiene previsto organizar para agentes de policía especializados en la materia períodos de formación a nivel paneuropeo, así como conferencias a alto nivel para mandos policiales, jueces y fiscales. Estas medidas tienen por objeto aumentar la sensibilización sobre el fraude de los medios de pago y su impacto en el sistema financiero.

Reorganizar el grupo de expertos en materia de prevención del fraude de cara a la ampliación de la Unión

La Comisión propuso que en cada país o sector actúe de contacto un experto en prevención del fraude que dé parte de los progresos realizados por el grupo a nivel nacional. La Comisión propone asimismo que se cree un grupo de control que prepare los trabajos del GEPF y supervise las actividades de los subgrupos de modo que se garantice la eficacia de las medidas previstas y se puedan celebrar reuniones con frecuencia. Propone también la Comisión que se creen un par subgrupos que aborden los problemas de seguridad y los relacionados con los usuarios. El GEPF debe asimismo propiciar una mejor comunicación con los ciudadanos y los profesionales del sector dando notoriedad a los progresos realizados y a la eficacia de las medidas del nuevo plan de acción.

Reforzar la seguridad de los sistemas de pago e implicar a los ciudadanos

La utilización de las tarjetas inteligentes refuerza la seguridad y reduce el riesgo de fraude. La Comisión sigue con especial interés cualquier nueva solución que redunde en aras de la seguridad y se muestra a favor de esta evolución. Concretamente, desea que se concite la confianza de los ciudadanos ofreciéndoles una mejor información sobre los niveles de seguridad. Los ciudadanos de la Unión tienen que disponer de una información más clara sobre la seguridad de los pagos y los comerciantes deben contar con un mejor material pedagógico y de instrumentos adecuados para protegerse de la piratería de los datos.

Hay tener en cuenta las evoluciones técnicas

Hay que mejorar la notificación de las pérdidas y robos de tarjetas de pago en la UE. Técnicamente es factible y deseable que los números para notificar la pérdida o el robo de una tarjeta sean los mismos en toda la UE. La Comisión ha previsto además una serie de iniciativas concretas para prevenir la usurpación de la identidad en la Unión, con frecuencia relacionada con la delincuencia organizada.

6. Mejoras y retos pendientes para la protección de los usuarios en la última normativa europea

(Directiva 2007/64 sobre servicios de pago)

La Directiva 2007/64/CE del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior, modifica la anterior Directiva 97/5/CE. Esta Directiva tiene como objetivo instaurar el marco jurídico necesario para la creación de un mercado de pagos integrado, es decir, la finalidad de impulsar en Europa un área de pago unificado mediante la implantación del SEPA (Single Euro Payments Area, cuyo objetivo es extender al ámbito de los pagos electrónicos la unidad monetaria efectiva que ya existe en el ámbito de monedas y billetes. Por último, y como consecuencia, **pretende establecer un nivel de protección en materia de información y a la definición de los derechos y obligaciones de los usuarios y de los proveedores de servicios de pago.**

Crítica a las “normas blandas”

Esta Directiva comienza con una autocrítica hacia las soluciones planteadas hasta ahora por la UE en materia de medios de pago y regulación de sus condiciones. En particular, en el considerando 3º dice expresamente:

“Las diferentes disposiciones comunitarias ya adoptadas en este ámbito, a saber, la Directiva 97/5/CE del Parlamento Europeo y del Consejo, de 27 de enero de 1997, relativa a las transferencias transfronterizas y el Reglamento (CE) n.º 2560/2001 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2001, sobre los pagos transfronterizos en euros, no han remediado suficientemente esta situación, como tampoco lo ha hecho la Recomendación 87/598/CEE de la Comisión, de 8 de diciembre de 1987, sobre un código europeo de buena conducta en materia de pago electrónico (relaciones entre financieros, comerciantes-organismos prestadores de servicios y consumidores), la Recomendación 88/590/CEE de la Comisión, de 17 de noviembre de 1988, relativa a los sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjetas o la Recomendación 97/489/CE de la Comisión, 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. Estas medidas siguen siendo insuficientes. Además la coexistencia de disposiciones nacionales y un marco comunitario incompleto da lugar a confusiones y a la ausencia de seguridad jurídica”.

En concreto, respecto de la cuestión que nos afecta, la Directiva introduce derechos y obligaciones de los usuarios y de los proveedores de servicios de pago.

Dice el considerando 20, “Dado que los consumidores y las empresas no están en la misma posición, no deben disponer del mismo nivel de protección. Si bien procede garantizar los derechos de los consumidores mediante disposiciones con respecto a las cuales no pueden establecerse excepciones en los contratos...” Lo que en principio supone un claro avance respecto a la situación actual, basada, como hemos visto, en la adopción de “normas blandas” y autorregulación.

Dentro de las normas contempladas en este bloque cabe destacar las siguientes:

Plazo de ejecución de las operaciones de pago:

La Directiva reduce considerablemente **los plazos de ejecución permitidos en la actualidad que pasarán a ser de D+1**. Siendo D el día de recepción de la orden por el proveedor de servicios del ordenante, el importe de la operación deberá ser abonado en la cuenta del proveedor de servicios del beneficiario antes del final del día hábil siguiente.

Para todos los demás pagos, se aplicarán por defecto si no existe acuerdo entre el usuario y el proveedor, aunque la capacidad de negociación de las partes está limitada en operaciones intracomunitarias, donde no se podrá acordar un plazo superior a cuatro días. Durante un período transitorio, que se extiende hasta el 1 de enero de 2012, el ordenante y su proveedor de servicios de pago podrán acordar un plazo diferente, no superior a tres días.

Fecha valor y disponibilidad de los fondos:

En cuanto a la fecha valor, la Directiva sobre servicios de pago ha procedido tanto a reducir los plazos, como a unificarlos para los diferentes tipos de operaciones, diferenciando únicamente entre los abonos y los adeudos:

a) abonos, la fecha de valor no puede ser posterior al día hábil en que se producen, es decir, ha de coincidir fecha de abono y fecha de valor; y

b) adeudos, la fecha de valor no puede ser anterior al momento en que el importe se cargue en la cuenta, es decir podrá ser el mismo día o posterior.

Finalmente, la cantidad de la operación de pago deberá estar a disposición del beneficiario tan pronto como haya sido abonada en la cuenta de su proveedor de servicios.

Responsabilidad del proveedor de servicios de pago en caso de no ejecución o de ejecución defectuosa de una operación de pago:

Se considera a este último objetivamente responsable, salvo circunstancias excepcionales e imprevisibles. La carga de la correcta ejecución de la operación recae en el proveedor de servicios.

Precaución del usuario

Responsabilidad del usuario de servicios de pago: en caso de utilización fraudulenta de un instrumento de pago la responsabilidad del usuario (excluidos los empresarios) estará limitada a **150 euros**. La Directiva prevé **dos excepciones** a la limitación de la responsabilidad en los términos expuestos, en función de la actuación del usuario:

a) actuación fraudulenta; o

b) incumplimiento, deliberado o por negligencia grave, de sus obligaciones. Hay que advertir no obstante que la Directiva da opción a los estados miembros a reducir esta cifra.

Gastos e importe íntegro

■ Criterio «SHARE»: **la Directiva prevé el reparto de los gastos ocasionados por la operación de pago entre el ordenante y el beneficiario**, debiendo hacerse cargo cada usuario de los gastos cobrados por su proveedor. Este criterio cambia totalmente para nuestro país, donde era el ordenante el que asumía los costes. Por otro lado, **debería haberse aprovechado para incluir una regulación más concisa** del ámbito de las comisiones financieras en los medios de pago.

■ Introducción del principio del importe íntegro: en virtud del cual **deberá abonarse en la cuenta del beneficiario el importe íntegro transferido por el ordenante**, sin deducciones por parte de ninguno de que el beneficiario y su proveedor de servicios pueden acordar que éste deduzca sus propios gastos del importe transferido antes de abonárselo al beneficiario, en cuyo caso habrán de figurar por separado el importe de la operación y sus gastos.

Condiciones de rectificación:

Según las cuales el usuario de servicios de pago tiene la **posibilidad de rectificar una operación** de pago no autorizada o ejecutada incorrectamente siempre que lo notifique a más tardar a los **13 meses** de la fecha del adeudo, aunque existe posibilidad de convenir otro plazo entre las partes.

Derecho de bloqueo del instrumento de pago:

Se considera expresamente la posibilidad de reserva del derecho de bloqueo del instrumento bajo razones objetivas. Dentro de las razones que permiten al proveedor de servicios bloquear el instrumento de pago se encuentran aquellas relacionadas con:

a) la seguridad del instrumento;

b) la sospecha de una utilización no autorizada o fraudulenta de dicho instrumento; o

c) en caso de que el instrumento esté asociado a una línea de crédito, como ocurre en las tarjetas de crédito, si aumenta el riesgo de que el ordenante sea incapaz de hacer frente a su obligación de pago.

Devoluciones de operaciones de pago iniciadas por el beneficiario o a través del mismo:

La Directiva va a establecer nuevos plazos y condiciones para proceder a cualquier tipo de devolución de operación de pago iniciada por el beneficiario o a través de él. En concreto se requiere que en las operaciones se cumplan dos condiciones: «a) cuando se dio la autorización, ésta no especificaba el importe exacto de la operación de pago; y b) el importe de la operación de pago supera el importe que el ordenante podía esperar razonablemente teniendo en cuenta sus anteriores pautas de gasto, las condiciones de su contrato marco y las circunstancias pertinentes al caso».

Estas condiciones son un requisito para todas las operaciones de pago iniciadas por el beneficiario o a través de él, a excepción de los adeudos domiciliados, donde pueden excluirse si así lo convienen el ordenante y su proveedor de servicios. En tal caso, el usuario tendrá derecho a devolución en todo caso.

También se prevé la posibilidad de negar el derecho de devolución cuando el ordenante haya dado su consentimiento y el proveedor de servicios o el beneficiario pongan a su disposición la información de la futura operación de pago con cuatro semanas de antelación.

El plazo para solicitar la devolución por operaciones iniciadas por un beneficiario o a través de él se aumenta considerablemente y pasa a ser de **ocho semanas** a partir de la fecha del adeudo. El proveedor debe proceder a la devolución en un plazo de 10 días o bien justificar su denegación de devolución, con indicación del organismo al que podrá dirigirse el ordenante si no acepta tal justificación.

Momento de irrevocabilidad:

La Directiva fija el momento en que una orden de pago deviene irrevocable dependiendo de su modalidad (ej: en las operaciones de pago convencionales, será el momento de recepción de la orden por el proveedor de servicios del ordenante, y en los adeudos domiciliados, al final del día anterior hábil al día de adeudo convenido). Con posterioridad a dicho momento, el proveedor de servicios podrá cobrar los gastos de la revocación si ésta fuera posible, para lo cual se exigirá con carácter general que se prevea esta posibilidad en el contrato marco y, en algunos supuestos, la concurrencia del acuerdo del beneficiario.

COSTES ELEVADOS PARA LOS USUARIOS DE TARJETAS

(Informe de la DG Competencia de la Comisión Europea sobre los servicios financieros a minoristas, 31 de enero de 2007)

La Comisión Europea publicó el informe final de su investigación de competencia en el sector bancario minorista. La investigación constató la existencia de varios problemas en los mercados de tarjetas de pago.

Los problemas de costes en Tarjetas de pago y sistemas de pago

■ **Grandes variaciones en las comisiones interbancarias en la UE**, que pueden no ser repercutidas completamente para permitir unas comisiones inferiores para los titulares de tarjetas. La Comisión no preconiza unas comisiones nulas, pero la forma de practicar estas comisiones en ciertas redes de pago es preocupante. Hay que recordar que las "tasas de intercambio" se abonan por la entidad que dota a un comercio de una TPV (Terminal de Punto de Venta) a la entidad que emitió la tarjeta empleada en la compra. Este Informe puso de manifiesto su relevancia de cara a establecer el resto de precios, tanto la tasa de descuento a los comerciantes, como las comisiones a los usuarios finales. Igualmente en el informe se refleja que las tasas de intercambio no son intrínsecas al funcionamiento de los pagos con tarjeta puesto que hay países que funcionan sin ellos, de hecho, afirmaba este Informe, las tarjetas de crédito son rentables incluso sin tasas de intercambio, poniendo en tela de juicio la DG Competencia la necesidad final de la tasa de intercambio.

■ **Alta y continua rentabilidad, particularmente en la emisión de tarjetas**, lo que sugiere que los bancos de algunos Estados miembros gozan de un importante poder de mercado y pueden imponer altas comisiones a las empresas y consumidores.

Después de la publicación del informe provisional sobre tarjetas y sistemas de pago, la Comisión se reunió con bancos de varios Estados miembros para estudiar cómo la autorregulación podría contribuir a solucionar los problemas de competencia. Una vez más la solución queda al arbitrio de la autorregulación, sin que los destinatarios últimos, los consumidores, a través de sus asociaciones legítimas, puedan participar en el diálogo en pie de igualdad.

Pese a todo, la Directiva de servicios de pago y su futura Ley en España, son insuficientes

No obstante esta Directiva 2007/64 sobre servicios de pago en el Mercado Interior (así como su norma de transposición al ordenamiento español, cuyo proyecto de ley de Servicios de Pago publicado en el Boletín Oficial de las Cortes Generales de 17 de abril de 2009), plantea numerosos interrogantes para los consumidores.

El principal de ellos es que la propia regulación contenida en esta Directiva remite muchas cuestiones, importantes para los derechos de los consumidores, al “acuerdo y convenio entre las partes”. Hay que advertir que los consumidores mantienen una posición de desequilibrio en sus relaciones tradicionales a la hora de contratar un producto o servicio. Este desequilibrio se agudiza notablemente cuando nos situamos en el ámbito de contratación tan complejo como el de los servicios financieros. Así, puede comprenderse fácilmente que los consumidores no “convienen ni negocian” los contratos, sino que por definición se limitan a aceptar las condiciones impuestas por bancos y cajas de ahorros a través de los llamados “contratos de adhesión”, que incluyen cláusulas y condiciones que dispuestas unilateralmente por la empresa oferente.

Así, la Directiva (y el proyecto de Ley) “permite” que se “negocie” aspectos trascendentes: gastos por comunicar información en determinado supuestos (artículo 32.2 de la Directiva); plazo de resolución con preaviso (artículo 45.1); modificación de las condiciones del contrato (artículo 44); excepciones a los derechos y obligaciones en las prestaciones de servicios de pago (artículo 51 y 53); gastos aplicables (artículo 52); consentimiento o retirada del mismo (artículo 54); límites a la utilización del instrumento de pago (artículo 55); obligaciones del proveedor del servicio de pago (artículo 57); devolución de operaciones de pago iniciadas por el beneficiario (artículo 62); solicitudes de devolución (artículo 63)... y así hasta superar la veintena de cuestiones. Parece lógico pensar que los consumidores no podrán “negociar ni convenir” estas cuestiones, ya que vendrán interpuestas en los contratos por las entidades proveedoras de servicios de pago.

7. Importancia de las Asociaciones de Consumidores (Dictamen del Comité Económico y Social Europeo sobre “La lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo”. 23 de octubre de 2008)

En este Dictamen, el Comité Económico y Social Europeo se lamenta de que las iniciativas emprendi-

das hasta la fecha para prevenir y luchar contra el fraude y la falsificación de medios de pago distintos del efectivo no hayan resultado suficientes para atajar la difusión de este fenómeno. Si bien se ha mejorado y reforzado el marco jurídico comunitario, todavía **no se han desarrollado plenamente ni el intercambio de información entre las entidades públicas y privadas, ni la cooperación eficaz entre las autoridades competentes de los Estados miembros.**

Hay que mejorar la relación entre países

Según este Dictamen, el principal obstáculo para lograr la aplicación eficaz de un sistema de prevención en la lucha contra el fraude reside en la dificultad de intercambiar datos sobre los ámbitos de actuación fraudulenta o de riesgo dentro de la Unión Europea. Para garantizar una acción preventiva eficaz, parece necesario por tanto, aumentar las modalidades de intercambio de información sobre los ámbitos de actuación fraudulenta mediante una mejora de los canales de cooperación entre las autoridades competentes de los Estados miembros.

Hacia una norma homogénea

Otro aspecto que limita la acción eficaz en la lucha contra el fraude, según este Dictamen, lo constituyen tanto la falta de homogeneidad en la legislación que regula el ejercicio de las atribuciones de instrucción por parte de cada administración nacional, como las diferencias en la intensidad de las medidas represivas. Así pues, la exigencia de llevar a cabo una verdadera aproximación de las legislaciones nacionales parece ser la principal línea de actuación para atajar eficazmente el fraude en este sector, que representa un fenómeno delictivo de carácter típicamente transnacional.

Campañas informativas europeas

Es importante señalar que el **Comité Económico y Social Europeo destaca la necesidad de emprender campañas informativas de gran difusión a través de las asociaciones de consumidores**, con vistas a llamar la atención de los usuarios sobre las posibles pautas de riesgo derivadas del uso de instrumentos de pago distintos del efectivo, a fin de lograr una participación consciente que permita luchar de manera eficaz y oportuna contra el fraude. Y es que, la multiplicación de éstos puede repercutir negativamente en la confianza que tienen depositada los consumidores en los sistemas de pago y se considera que constituye uno de los principales obstáculos para el crecimiento del comercio electrónico.

La escasa normativa española que regula las transacciones con medios de pago distintos del efectivo

■ Regulación en el Código civil español

El CC establece los requisitos para los contratos en un ámbito general, sin hacer especial referencia a los contratos bancarios.

En el **Código de comercio** encontramos regulación sobre algunos medios de pago tradicionales. En el título X de esta norma se regulan las letras de cambio, En el XI los cheques y en el XII robo, hurto, extravío o falsedad de efectos al portador.

■ La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

En su artículo 248 los fraudes en medios de pago electrónico se reconocen como un **delito de estafa**.

En el primer párrafo de este artículo se regula el concepto tradicional de estafa, y en el segundo todas aquellas conductas defraudatorias llevadas a cabo mediante manipulaciones informáticas o estafas informáticas. Los principales elementos que se recogen en este segundo párrafo son: el ánimo de lucro, perjuicio a tercero y la transferencia no consentida del patrimonio de otra persona sin utilizar violencia.

En materia de estafas electrónicas el código penal, sólo hace una tipificación de las estafas con ánimo de lucro valiéndose de alguna manipulación informática, pero **no detalla las penas a aplicar en la comisión del delito**.

■ Transferencias bancarias

La ley aplicable a este medio de pago es la **ley 9/1999 de 12 de abril**, reguladora del régimen jurídico de las transferencias entre estados miembros de la UE. En concreto los artículos 5-9 regulan los casos de incumplimiento de plazos en las transferencias y las consecuencias derivadas del mismo. Los plazos estipulados son los mismos que establece la Directiva 97/5/CE.

■ Trasposición de la Directiva 2007/64/CE

Recientemente, el Gobierno ha aprobado el proyecto de ley que traspone la **Directiva 2007/64/CE** del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, con el fin de facilitar las operaciones de pago en el ámbito de la UE, reforzando los derechos y protección de los usuarios.

Con este proyecto de ley se traspone la Directiva comunitaria de 2007 con la que se pretende armonizar la regulación dispersa que sobre la materia tienen los distintos Estados miembros.

■ Pagos on línea

Aunque no existe normativa específica para este medio de pago, sí que encontramos normativa que hace alguna mención al respecto.

La ley 34/2002, de servicios de la sociedad de la información y comercio electrónico asegura la eficiencia de los contratos celebrados por vía electrónica, equiparando la forma escrita. En resumen lo que se pide es que el prestador de servicios ponga a disposición del usuario de forma permanente, fácil y gratuita, la información necesaria. Una vez celebrado el contrato el prestador de servicio deberá confirmar la recepción de la aceptación.

De todo lo expuesto cabe deducir que a pesar de que existe normativa específica para este campo, esta es relativa a la UE, siendo imprescindible una buena adaptación a la realidad nacional española.

Normativa europea sobre tipos penales comunes y cooperación judicial frente al fraude en medios de pago

Como se ha apuntado, a la hora de atajar los casos fraudulentos que se perpetran en el seno de la UE, la mayor limitación viene dada por la falta de homogeneidad en la legislación que regula el ejercicio de las competencias de instrucción por parte de las distintas administraciones nacionales, así como por la distinta intensidad de las medidas represivas. Así pues, hay que establecer una tipificación penal en los Estados miembros de estos delitos, castigados con sanciones efectivas y disuasorias que permitan penar el fraude cometido con tarjetas de pago. De lo contrario, los casos de fraude se producirían en aquellos países donde las competencias de inspección de los organismos responsables de los controles son más reducidas o donde las sanciones aplicables resultan inadecuadas para desempeñar su función de prevención. La exigencia de una aproximación de las legislaciones nacionales parece ser la única estrategia para atajar eficazmente el fraude en este sector.

1. Una buena herramienta de trabajo debe cumplirse

(Consejo de Europa: Convenio sobre Cibercrimen de 23 de noviembre de 2001)

Las dificultades basadas en la vinculación territorial a la persecución de los ilícitos penales hacen ver inmediatamente la necesidad de una armonización legislativa y la cooperación internacional en esta materia, sin las que no se puede proporcionar una respuesta eficaz a esta nueva forma de criminalidad. El principal instrumento frente a las limitaciones por falta de armonización de las legislaciones y por la falta de mecanismos para la investigación penal fuera del territorio propio, en la actualidad es la Convención sobre Cibercriminalidad del Consejo de Europa de 23.11.2001. Se trata de un texto firmado por más de una treintena de países de todo el mundo todavía que a fecha de hoy sigue un lento proceso de ratificaciones. A pesar de la lentitud en la ratificación de los distintos países y de su puesta en práctica representa el instrumento internacional de la lucha contra la delincuencia informática más destacado.

Abarca el fenómeno de la delincuencia informática desde múltiples ópticas. En el mismo se incluyen medidas que los Estados deben adoptar en sus legislaciones nacionales, tanto en lo relativo a Derecho penal como a Derecho procesal penal. Las medidas de derecho penal material consisten en la armonización de las distintas legislaciones penales de los países signatarios mediante la incorporación al derecho interno de las figuras penales que recoge la Convención.

El Convenio de Cibercrimen propone entonces, en esta materia, varias infracciones que deberán ser incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales, algunos de los cuales poseen especial incidencia en los supuestos relativos a los abusos con medios electrónicos de pago.

Protección de la confidencialidad

Un primer grupo de infracciones lo constituyen los hechos contrarios a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Dentro de este grupo se incluyen las conductas de acceso ilegal injustificado a todo o parte de un sistema informático. (art. 2).

De momento la legislación penal actual española, a diferencia de lo que sucede en otros países, como Portugal, no conoce una auténtica infracción de mero acceso o mero intrusismo informático. De todas formas el Convenio permite que las partes firmantes modulen la incriminación de este supuesto mediante diferentes formas. Así es posible vincular la incriminación de este supuesto mediante diferentes formas. Así es posible vincular la punibilidad de este hecho a la violación de medidas de seguridad, la existencia en el autor de determinadas intenciones a la hora de realizar el hecho, o la presencia de conexión entre distintos sistemas informáticos.

También se abarcan los supuestos de Interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior de un mismo sistema, mediante el empleo de medios técnicos (art. 3). En el art. 4 se sitúan los atentados a la integridad de los datos, consistente en el daño, borrado, deterioro, alteración o supresión intencional de datos informáticos. Este supuesto último se puede condicionar a la producción de daños de carácter grave. La interceptación así como la lesión de la integridad de los datos, podrán poseer aplicación, especialmente en relación a los ilícitos previstos en los documentos de la UE, cuando los datos tienen que ver con una transferencia electrónica de fondos.

Una mayor novedad para el sistema español, representa el caso de los atentados a la integridad de los sistemas, consistente en el entorpecimiento grave de un sistema informático mediante las conductas anteriores

de introducción, transmisión de daño, borrado, deterioro o supresión de datos informáticos (art.5). Finalmente como hechos dignos de castigo por las legislaciones nacionales todo tipo de conductas abusivas relativas a los dispositivos informáticos (desde la producción y venta hasta la obtención para su utilización) que permiten la realización de los hechos delictivos anteriores.

Hacia un futuro delito de “fraude informático”

El segundo grupo de conductas las denomina el Convenio “Infracciones informáticas”, y en ellas se incluye la falsedad informática y el fraude informático, con evidente repercusión para los supuestos de delitos cometidos con o sobre medios electrónicos de pago. Falsificación informática del art.7 que resulta de la producción de datos informáticos o auténticos para su utilización con fines legales como si de datos genuinos se tratara. El fraude informático (art.8) hace referencia a las conductas de introducción, alteración, borrado o supresión de datos informáticos, o cualquier forma de atentado al funcionamiento de un sistema informático con la intención de obtener un beneficio económico para sí mismo o para otro. Se vincula entonces este supuesto a las actuaciones fraudulentas en los sistemas informáticos que persiguen el enriquecimiento injusto.

Protección también a los datos personales

También se incluyen medidas de derecho Penal, de forma que los países deben incorporar a sus procedimientos penales determinados contenidos, como la necesidad de conservación de datos y protección de la integridad de datos almacenados, así como para la comunicación de los datos de tráfico a las autoridades competentes. Igualmente el derecho interno debe proporcionar los instrumentos legales necesarios para que se pueda ordenar la comunicación a las autoridades de datos informáticos controlados por una determinada persona así como los datos de los abonados en relación a la prestación de determinados servicios, el acceso durante la investigación a los datos o la obligación de registrar determinados datos relativos al tráfico por parte de los prestadores de servicios, así como la interceptación de datos relativos al contenido. Todo ello siempre con las condiciones y garantías de derecho interno en relación a las investigaciones por infracciones penales y con supervisión judicial o de autoridades independientes (arts. 14 y 15 del texto).

La cooperación internacional es clave

Resultan fundamentales las medidas de cooperación internacional previstas en la Convención. La Convención hace las veces de tratado de extradición para el caso de partes que tengan suscrito alguno y establece las condiciones mínimas que faciliten los procedimientos de extradición entre las partes firmantes en relación a los delitos que son objeto de incriminación.

Se establecen medidas de ayuda mutua entre los firmantes para los fines de investigación o procedimientos concernientes a infracciones recogidas en la Convención. Se realizarán valiéndose de los prestadores de servicios de cada país y mediante el establecimiento de autoridades nacionales de cada estado que canalicen las comunicaciones de cada estado. Esta Convención establece la posibilidad de asistencia mutua en las investigaciones de las infracciones y obtención de pruebas, así como para el establecimiento de medidas cautelares. Se prevé la posibilidad de solicitar a alguna de las partes la conservación de datos de tráfico, el acceso a los datos almacenados, así como la interceptación de datos relativos a tráfico y contenido.

2. Un marco jurídico común para luchar contra el fraude en medios de pago

(Libro Verde sobre la aproximación, el reconocimiento mutuo y la ejecución de penas en la Unión Europea Bruselas, 30 de abril de 2004)

La Unión Europea se ha fijado como objetivo ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia (artículo 29 del Tratado de la Unión Europea). Desde esta perspectiva, la Comisión consideró pertinente analizar si las diferencias nacionales en materia de penas constituyen un obstáculo a la realización de este objetivo, y en particular en las operaciones fraudulentas en medios de pago, al tiempo que opina que sería asimismo necesario examinar si esas diferencias plantean problemas a la cooperación judicial entre los Estados miembros, lo que en primer lugar supondría señalar los obstáculos existentes a la aplicación del principio del reconocimiento mutuo, que, según las conclusiones del Consejo Europeo de Tampere, debe convertirse en «la piedra angular» del funcionamiento de la Unión en materia de justicia y, en general, ha de facilitar la ejecución en un Estado miembro de las penas impuestas en otro.

Enorme diversidad entre Estados miembros en materia penal

Las diferencias entre las legislaciones de los Estados miembros en materia de penas son, según este Libro Verde, bastante considerables. En efecto, los sistemas penales de Estados miembros están divididos por lo que se refiere a los principios de oportunidad y legalidad de la acción penal. El principio de oportunidad se aplica en Bélgica, Francia, Dinamarca, Irlanda, el Reino Unido, Luxemburgo y los Países Bajos. En Alemania, Austria, España, Finlandia, Suecia, Grecia, Italia y Portugal es el principio de legalidad el que se aplica.

De acuerdo con el principio de legalidad, las autoridades competentes para ejercitar la acción penal deben intervenir de oficio - y en consecuencia incluso

en ausencia de denuncia – cuando sospechen de la existencia de una infracción. Por el contrario, según el principio de oportunidad, la decisión de adoptar medidas contra la infracción se deja a la apreciación del fiscal.

Sin embargo, en la práctica, todos los sistemas jurídicos contienen elementos procedentes de ambos principios. Los que siguen el principio de legalidad aplican, en algunos casos, criterios de oportunidad, por ejemplo, la posibilidad de archivo de las actuaciones bajo condición, y los que se basan en criterios de oportunidad, admiten, por ejemplo, instrucciones de los Fiscales Generales u orientaciones de política criminal emanadas del Ministro de Justicia y se matizan, en particular, por la exigencia de motivación de las resoluciones por las que se archiva la causa y/o por la instauración de vías de recurso efectivas.

En el Reino Unido, por ejemplo, la oportunidad se basa en dos normas: la perspectiva razonable de obtener una condena - que cada vez se utiliza más en los países en los que se aplica el principio de legalidad - y el interés público. Por el contrario, en los sistemas en los que se aplica el principio de legalidad, existen criterios para dar prioridad a determinados asuntos y no enjuiciar penalmente casos menores.

La discrecionalidad del juez penal

Aunque se pretenda crear un espacio de libertad, seguridad y justicia en el que la misma infracción se sancione en todas partes de manera equivalente, lo cierto es que solo se puede jugar con los marcos legislativos que se proporcionan hasta cierto punto, mientras que el resultado concreto siempre estará en función de un factor desconocido: la decisión del juez que dispone, en todas partes, de un poder discrecional a la hora de imponer la pena.

Sin embargo, el primer límite a la libertad del juez en la imposición de la pena se deriva del principio fundamental de la legalidad de las penas, que le obliga, cuando considere que se ha cometido una infracción, a imponer la pena prevista por la ley para esta infracción. Esto se deriva del principio de seguridad jurídica, que exige que la pena correspondiente a una infracción venga especificada por la ley. La presencia de circunstancias agravantes y atenuantes puede también, hasta cierto punto, limitar la libertad del juez, así como, por ejemplo, la posibilidad de disminución de pena o las eximentes legales.

La aproximación de penas contribuye a la consecución de la compatibilidad de las normas aplicables en los Estados miembros, en la medida necesaria para facilitar la cooperación judicial penal y, por otra, a la facilitación y aceleración de la cooperación entre los ministerios y las autoridades judiciales o equivalentes competentes de los Estados miembros en relación con la ejecución de resoluciones.

Evitar el “Dumping penal” de las bandas

La aproximación de penas justas, razonables y disuasorias

La aproximación en el ámbito de las penas puede perseguir varios objetivos, combinados entre sí: En primer lugar, al establecer tipificaciones y penas comunes respecto de determinadas formas de delincuencia. La aproximación de penas contribuiría a dar a los ciudadanos un sentimiento común de justicia, una de las condiciones de la creación del espacio de libertad, seguridad y justicia.

Hay que definir perfectamente un tipo penal de fraude en medios de pago

Además, significaría claramente que ciertos comportamientos son inaceptables y se sancionan de una manera equivalente. Pensemos, por ejemplo, en un tipo único en materia de fraudes en medios de pago. La aproximación tanto en la tipificación de la conducta como en la gravedad de la pena que lleve aparejada conduce a una protección efectiva y equivalente de los ciudadanos en todo el territorio de la Unión frente a un fenómeno que se opone a los principios y valores comunes de los Estados miembros.

Sanciones idénticas en todo el espacio europeo

Por otra parte, el corolario de un espacio europeo de justicia sería que las mismas conductas criminales estuvieran sujetas a unas sanciones similares para su autor, cualquiera que fuere el lugar de comisión de la infracción en la Unión. Por lo tanto, la aproximación de las legislaciones constituye un objetivo autónomo, en aquellos ámbitos que se consideren prioritarios y se definen como tales.

EL primer paso, acercar las legislaciones de los distintos estados miembros

Cierto grado de aproximación de las disposiciones de Derecho penal material resulta necesario, en particular si se considera que algunas formas de delincuencia revisten una dimensión transnacional y los Estados miembros no pueden enfrentarse a ellas en solitario.

organizadas en fraudes en medios de pago

Unas normas mínimas de la Unión contribuyen asimismo a impedir que los delincuentes (o al menos algunas categorías de ellos como, por ejemplo, los de la delincuencia organizada) se aprovechen de que las penas son muy divergentes de un Estado a otro y se desplacen de uno a otro para eludir el procesamiento o la ejecución de las penas. Las conclusiones de Tampere (punto nº 5) destacan que debe evitarse que los delincuentes encuentren la forma de aprovecharse de las diferencias existentes entre los sistemas judiciales de los Estados miembros.

Si bien es cierto que la gravedad de las penas aplicables condicionaba la implantación de algunos mecanismos de cooperación judicial en materia penal, prácticamente ya no ocurre así a raíz de la adopción de instrumentos basados en el principio del reconocimiento mutuo.

Asimismo, existe un vínculo entre aproximación del Derecho penal y ejecución eficaz de una política de la Unión en un ámbito que haya sido objeto de medidas de armonización, pudiéndose citar, a título de ejemplo, las transacciones económicas y financieras como materias en las que el Derecho penal podría contribuir a garantizar el respeto de una política de la Unión.

Por último, la aproximación de las normas de Derecho penal sobre las penas y su ejecución contribuye a facilitar la aceptación del reconocimiento mutuo de las sentencias, puesto que refuerza la confianza mutua. La aproximación no es, sin embargo, una condición sine qua non del reconocimiento mutuo; se trata más bien de dos mecanismos complementarios mediante los que se puede alcanzar la realización del espacio judicial europeo. Por lo tanto, se facilitaría la compatibilidad de las normas aplicables en los Estados miembros y, por otra parte, se mejoraría con ello la cooperación entre las autoridades competentes de los Estados miembros en relación con la ejecución de resoluciones. Además, unas condiciones de ejecución de las penas compatibles entre los Estados miembros favorecerían la reinserción de

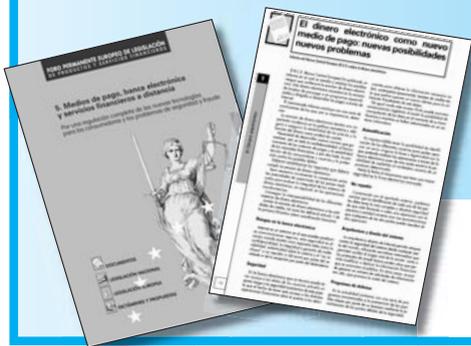
las personas y les permitirían purgar su pena en un Estado miembro distinto del de condena. Sin embargo, cualquier acción que tenga por objeto llevar a cabo una aproximación de las penas debe obviamente respetar los principios de subsidiariedad y proporcionalidad.

Sin un marco jurídico penal común es difícil contrarrestar los fraudes

La aproximación del Derecho penal material llevada a cabo a escala de la Unión sigue siendo muy limitada. En efecto, no se incluyen todos los ámbitos criminales y las tipificaciones son a veces explícitamente mínimas o contienen excepciones. Por otra parte, algunas conductas punibles no se definen en los instrumentos y se perciben de manera diferente en los Estados miembros (por ejemplo: tentativa, participación, inducción). Es preciso, asimismo, recordar que, por lo que se refiere a la aproximación de las penas, el ejercicio se ha limitado a establecer, por lo que a las sanciones aplicables se refiere, bien unas penas efectivas, proporcionadas y disuasorias, bien a fijar la duración mínima de la pena máxima. En efecto, además de la pena de prisión, existe un amplio abanico de sanciones previstas en los sistemas penales de los Estados miembros. Por otro lado, aun cuando se fije la misma pena aplicable a una infracción, existen importantes divergencias en las normas generales del Derecho penal de los Estados miembros que conducen a una diferencia entre la pena impuesta y la ejecutada (por ejemplo, por lo que se refiere a la investigación activa de los delitos, la aplicación del principio de legalidad u oportunidad del ejercicio de la acción penal, el grado de la pena impuesta y la pena realmente ejecutada).

Además, el arsenal de instrumentos de reconocimiento mutuo en la Unión Europea sigue siendo bastante incompleto. En particular, a este nivel, no existe prácticamente ninguna normativa sobre reconocimiento mutuo de penas privativas de libertad y de su ejecución en otro Estado miembro.

El dinero electrónico como nuevo medio de pago: nuevas posibilidades nuevos problemas



Por una legislación completa de las nuevas tecnologías para los consumidores y los problemas de seguridad y fraude

CONSIGA TODAS ESTAS
INTERESANTES Y
AMENAS
PUBLICACIONES

Llámenos: ADICAE

C./ Gavín, 12 local. 50001 ZARAGOZA

Tfno.: 976 390060 ■ Fax: 976 390199

email aicar.adicae@adicae.net

3. Combatir la delincuencia financiera organizada

(Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la prevención y la lucha contra la delincuencia organizada en el sector financiero, 2004)

Esta Comunicación tenía por objeto determinar los ámbitos en los que podrían ser necesarias nuevas iniciativas para reforzar la lucha contra la delincuencia financiera organizada. Este fenómeno abarca todo un abanico de actividades ilegales, concretamente el blanqueo de dinero, el fraude financiero y la falsificación del euro (donde podría incluirse los medios de pago distintos de efectivo) puesto que son obra de organizaciones criminales. La delincuencia financiera organizada perjudica a los agentes económicos legítimos e incrementa la economía sumergida, mermando así el crecimiento económico y los recursos públicos. Combatirla es importante ya que desempeña un papel, en términos más amplios, en la lucha contra la delincuencia organizada en general. Como este tipo de delincuencia está generada por el dinero, el hecho de impedir el acceso al mismo a los grupos criminales organizados no puede sino debilitarlos.

Medidas contra el fraude en pagos distintos del dinero

El fraude y la falsificación que se producen en los medios de pago distintos del dinero en efectivo representan una fuente importante de ingresos ilícitos para los grupos criminales organizados.

La Comisión destaca que es necesario llegar a nivel comunitario a una definición común y exhaustiva del fraude y a la armonización de las sanciones penales. La Comisión tiene la intención de lanzar un estudio comparativo de las distintas definiciones del fraude y sus consecuencias penales. El fraude a los intereses financieros de la Comunidad representa también una fuente importante de ingresos ilícitos, al tiempo que causa pérdidas enormes a los recursos propios de la UE. Para luchar contra este fenómeno, la Comisión recomienda:

- Reforzar la cooperación entre los Estados miembros, la Comisión, Eurojust y, en su caso, Europol;
- Designar un fiscal europeo independiente, encargado de detectar y perseguir las infracciones cometidas contra los intereses económicos de la Comunidad.
- El desarrollo de la cooperación entre el sector público y el sector privado, no sólo en el marco del foro de la UE sobre la prevención de la delincuencia organizada, sino también promoviendo la investigación en este ámbito. Asimismo, analizará también las posibilidades de coordinación entre, por una parte, los funcionarios de las fuerzas de seguridad y de la administración en general y, por otra, los representantes de los círculos

los financieros y económicos afectados por la delincuencia financiera organizada;

- La continuación de la puesta a punto de un mecanismo que permita localizar las propuestas legislativas que, por inadvertencia, podrían dar paso a maniobras criminales. En una etapa posterior, y si fuese necesario, la Comisión prevé hacer extensivo este método de evaluación del riesgo de delito, traspasando el proceso legislativo, a los procedimientos aplicables en ámbitos como las solicitudes de reembolso de siniestros o las solicitudes de tarjetas de crédito, para reducir las posibilidades de fraude;

- Una evaluación completa de la eficacia y el impacto de las políticas y medidas de lucha contra la delincuencia financiera organizada en la UE. El objetivo consistirá en determinar las mejores prácticas y los ámbitos en los que podrían adoptarse medidas adicionales contra este tipo de delitos;

- La prolongación de acciones como seminarios, talleres y estudios financiados gracias a su programa de financiación AGIS;

- El refuerzo de la acción exterior en la lucha contra la delincuencia financiera organizada a través de los programas de asistencia técnica dirigidos a los terceros países y la celebración de acuerdos con éstos.

4. Medidas para una competencia jurisdiccional común en fraudes en medios de pago

(La Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información)

En su artículo segundo establece que cada Estado adoptará las medidas necesarias para que sean castigadas como infracción penal, el acceso intencionado sin autorización a sistemas de información, la intromisión intencionada, y no autorizada, en sistemas de información a fin de obstaculizar o interrumpir de manera significativa el funcionamiento de los mismos.

La intromisión intencionada y no autorizada en datos informáticos contenidos en sistemas de información que produzcan el efecto de borrarlos, dañarlos, deteriorarlos, alterarlos, suprimirlos o hacerlos inaccesibles serán asimismo sancionadas.

La propuesta de penas de 1 a 5 años

En su empeño armonizador, la Decisión no sólo proclama que las sanciones penales habrán de ser efectivas, proporcionadas y disuasorias, sino que las sanciones más graves estarán comprendidas entre uno a tres años de prisión como mínimo en su grado máximo.

La sanción será de dos a cinco años de prisión como mínimo en su grado máximo cuando se cometan en el marco de una organización delictiva tal como la define la Acción Común 98/733/JAI83. Esta circunstancia agravante podrán contemplarla los Estados miembros si la infracción hubiera ocasionado graves daños o afectado a intereses esenciales. Cuando el delincuente sea una persona jurídica, y con independencia de la sanción que corresponda a las personas físicas que la administren, podrán imponerse contra aquélla sanciones, penales o administrativas, de naturaleza económica o incluso la vigilancia de las actividades.

Esta decisión se refiere por primera vez a la competencia jurisdiccional

Al Estado en cuyo territorio se haya cometido, total o parcialmente la infracción, que comprende tanto el caso en que el infractor se encuentre físicamente en ese Estado aunque el ataque se produzca en sistemas informáticos situados en otro país, como el supuesto inverso, es decir, cuando el autor se halle físicamente en otro país pero la infracción se cometa en sistemas informáticos situados en el Estado de que se trate.

También tendrá jurisdicción cualquier Estado de la UE para conocer del asunto cuando la infracción la hubiese cometido uno de sus nacionales y, asimismo, el Estado en cuyo territorio tenga su domicilio social la persona jurídica en cuyo beneficio se comete la infracción.

Bastaría la comisión parcial del delito para que un Estado aplicara su jurisdicción, siendo frecuentes los multiaques informáticos que producirían la potencial actuación de muchas jurisdicciones. Los Estados que persiguiesen a sus nacionales podrían colisionar con la jurisdicción de aquellos en cuyo territorio se ha cometido el delito o en cuyo territorio se domiciliase la persona jurídica administrada por el nacional perseguido por su propio país.

La Decisión Marco dispone que cuando una infracción sea competencia de más de un Estado miembro y cualquiera de estos Estados pueda legítimamente iniciar acciones judiciales por los mismos hechos, los Estados miembros de que se trate colaborarán para decidir cuál de ellos iniciará acciones judiciales contra los autores de la infracción, con el objetivo de centralizar, en la medida de lo posible, dichas acciones en un solo Estado miembro.

Con este fin, los Estados miembros podrán recurrir a cualquier órgano o mecanismo creado en el marco de la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de sus actuaciones.

Para determinar a qué Estado corresponderá finalmente el ejercicio de la jurisdicción, se podrán tener en cuenta consecutivamente los siguientes criterios:

- 1) El Estado miembro en cuyo territorio se hayan cometido las infracciones.
- 2) El Estado miembro del que sea nacional el autor.
- 3) El Estado miembro en el que se haya encontrado al autor.

5. Una buena herramienta para intercambiar información sobre el cibercrimen

(Plan de acción plurianual 2009-2013 relativo a la justicia en red Europea)

Como hemos visto, uno de los requisitos exigidos para luchar contra el fraude en medios de pago es la necesidad de cooperación entre Estado y organismos, así como el intercambio de información. La justicia en red europea tiene por objeto favorecer la creación de un espacio de justicia europea utilizando las tecnologías de la

El "EURO" de los medios de pago

El proyecto de la Zona Única de Pagos para los países del Euro (SEPA) forma parte integrante del proceso de creación de un mercado único financiero en Europa. Su objetivo es crear un área única de pagos para operaciones bancarias como transferencias, tarjetas... ADICAE participa en los procesos de creación de normas que afectan a los consumidores en este ámbito.

CONSIGA TODAS ESTAS
INTERESANTES Y
AMENAS
PUBLICACIONES

Llámenos: ADICAE
C./ Gavín, 12 local. 50001 ZARAGOZA
Tfno.: 976 390060 ■ Fax: 976 390199
email aicar.adicae@adicae.net



información y la comunicación. En este contexto, las actuaciones realizadas en el marco de la justicia en red europea deben participar potencialmente todos los Estados miembros de la Unión Europea. Además, la justicia en red europea constituirá un instrumento de trabajo para las autoridades judiciales, facilitando una plataforma y funcionalidades individuales para intercambios de información eficaces y seguros.

Facilitar el acceso a la justicia

En junio de 2007, el Consejo decidió que deberían emprenderse trabajos para desarrollar, a escala europea, la utilización de tecnologías de la información y la comunicación (TIC) en el ámbito de la justicia, en particular mediante la creación de un portal europeo. Efectivamente, la utilización de estas nuevas tecnologías contribuye a la racionalización y la simplificación de los procedimientos judiciales. La utilización de un sistema electrónico en este ámbito permite reducir los plazos de los procedimientos y los costes de funcionamiento, en beneficio de los ciudadanos, las empresas, los profesionales del Derecho y la administración de justicia. Se facilita por tanto el acceso a la justicia.

Las cuestiones relativas a la justicia en red no se limitan a determinados ámbitos jurídicos. Se plantean en numerosos ámbitos del Derecho civil, penal y administrativo. La justicia en red es pues una cuestión horizontal en el marco de procedimientos europeos de carácter transfronterizo.

Funciones de la justicia en red europea

Los trabajos llevados a cabo por el Grupo «Justicia en red» y la Comunicación de la Comisión permiten definir con claridad las funcionalidades del futuro sistema de justicia en red europea. Deberán establecerse las tres funciones esenciales siguientes:

a) Acceso a la información correspondiente al ámbito de la justicia. Dicha información se refiere, en particular, a la legislación y a la jurisprudencia europeas así como a las de los Estados miembros. La Justicia en red europea dará también acceso, mediante interconexiones, a la información gestionada por los Estados miembros en el marco del servicio público de la justicia (por ejemplo, y a reserva de las normas de funcionamiento, la interconexión de las bases de datos del registro de antecedentes penales de los Estados miembros).

b) Desmaterialización de los procedimientos. La desmaterialización de los procedimientos judiciales y extrajudiciales transfronterizos (por ejemplo, la mediación en red) engloba concretamente la comunicación electrónica entre un órgano jurisdiccional y las partes interesadas, en particular mediante la aplicación de los instrumentos europeos adoptados por el Consejo.

c) Comunicaciones entre autoridades judiciales. Presentan especial importancia la simplificación y la promoción de las comunicaciones entre las autoridades judiciales de los Estados miembros, especialmente en el

marco de los instrumentos adoptados en el espacio judicial europeo (por ejemplo, mediante videoconferencia o una red electrónica segura).

Una vez conocidos los trabajos y las líneas de actuación de la Unión Europea en materia de coordinación penal y cooperación judicial, vamos a conocer, en el capítulo siguiente cómo trata nuestra doctrina la cuestión penal en España de los fraudes en medios de pago.

6. El tratamiento procesal penal del cibercrimen

La falta de regulación específica en esta materia supone que haya que recurrir a normas sobre la asistencia judicial penal en la Unión Europea y a las normas reguladoras de las actuaciones conjuntas entre fuerzas de seguridad de varios Estados. Las menciones específicas del cibercrimen son escasas y están sujetas a diversas interpretaciones.

El Convenio sobre asistencia judicial en materia penal en la Unión Europea

El Convenio relativo a asistencia judicial en materia penal entre los Estados miembros de la Unión Europea resulta de aplicación al cibercrimen, sin embargo, ha de complementarse con los instrumentos internacionales y transnacionales que en el momento de su aplicación existan.

El Convenio pretende activar la ayuda mutua entre autoridades judiciales, policiales y aduaneras de los Estados miembros, completando y facilitando la aplicación del Convenio de 1959 del Consejo de Europa sobre ayuda mutua en materia penal y de su protocolo de 1978, del Convenio de aplicación del Acuerdo de Schengen de 1990 y del Tratado Benelux de 1962, de forma compatible con los principios fundamentales de sus respectivos Derechos internos, respetando los derechos individuales y los principios contenidos en el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, firmado en Roma el 4 de noviembre de 1950.

El Convenio contempla el traslado temporal de detenidos; la intervención de testigos o peritos a través de videoconferencia en procedimientos incoados en otros Estados miembros; la creación de equipos comunes de investigación entre dos o más estados miembros; las investigaciones encubiertas, mediante la intervención de agentes que utilicen una identidad secreta o ficticia y la interceptación de telecomunicaciones.

Equipos conjuntos de investigación

Cuando la investigación de infracciones penales en un Estado miembro requiera investigaciones difíciles que impliquen la movilización de medios considerables y afecten también a otros Estados miembros; cuando varios Estados miembros realicen investigaciones sobre in-

fracciones penales que requieran una actuación coordinada y concertada de los Estados miembros afectados; ofrece las pautas y condiciones para la creación de los equipos comunes, su constitución, la dirección, el alcance de la intervención de los “destinados” extranjeros en el país donde actúe el equipo, etc

Excepcionalmente se prevé la posibilidad de que tomen parte en los equipos funcionarios de organismos creados de conformidad con el Tratado de la Unión Europea, en la medida en que lo permitan la legislación de los Estados miembros interesados o las disposiciones de todo instrumento jurídico aplicable entre ellos.

El Convenio, que simplifica burocráticamente la cooperación transnacional, acompañado de la adecuada diligencia policial y judicial, podría constituir un válido instrumento para responder a la delincuencia informática, donde el carácter transnacional de las conductas hace muy difícil no ya su descubrimiento, sino su castigo, siendo frecuentes los problemas de jurisdicción competente.

Conclusiones en el ámbito europeo: la colaboración entre estados y la cooperación entre entidades financieras y Asociaciones de consumidores y usuarios, son claves para frenar el fraude en medios de pago

■ *Pese a tener una moneda única, los consumidores europeos no disponemos de un sistema de medios de pago único, justo y seguro*

La multiplicación de fraudes en medios de pago repercute negativamente en la confianza que tienen depositada los consumidores en los sistemas de pago y se considera que constituye uno de los principales obstáculos para el crecimiento del comercio electrónico.

■ *Insuficiente normativa*

Las declaraciones, recomendaciones, acuerdos, etc. adoptadas desde distintas instituciones europeas, así como las decisiones tomadas por los distintos Estados miembros, avanzan a un paso más lento que la realidad, lo que está permitiendo que los fraudes en medios de pago se conviertan en un hecho recurrente.

■ *Mayor colaboración entre operadores de mercado y sociedad civil*

Una de las cuestiones que se evidencia más claramente es la necesidad de que la relación entre actores privados (empresas) públicos (instituciones europeas) y ciudadanos (consumidores y usuarios) sea más intensa.

■ *Cooperación para la regulación*

Esta mayor vinculación debe plasmarse en una mejora en la cooperación entre organizaciones sociales (asociaciones de consumidores y usuarios) a la hora de establecer los mecanismos de regulación y control. Asimismo, debe contarse con estas organizaciones para difundir de una manera efectiva y eficaz, los riesgos en los medios de pagos y, sobre todo, los mecanismos para paliarlos de manera razonable y con las mínimas repercusiones para los consumidores.

■ *Fomento de la educación e información*

Necesidad de emprender campañas informativas de gran difusión a través de las asociaciones de consumidores, con vistas a llamar la atención de los usuarios sobre las posibles pautas de riesgo derivadas del uso de instrumentos de pago distintos del efectivo, a fin de lograr una participación consciente que permita luchar de manera eficaz y oportuna contra el fraude.

■ *Acabar con la autorregulación y acercar las disposiciones normativas*

La armonización de las disposiciones contractuales que regulan la relación entre los emisores y los titulares de las tarjetas y de las que regulan las modalidades para efectuar los pagos, la mayor limitación viene dada por la falta de homogeneidad en la legislación que regula el ejercicio de las competencias de instrucción por parte de las distintas administraciones nacionales.

Parte 3

La regulación y control penal en España: Luces y sombras en la lucha contra el fraude en medios de pago



El desarrollo de nuevas herramientas tecnológicas ha permitido la implantación de nuevas tecnologías de la comunicación, influyendo notablemente en la vida cotidiana de los consumidores. Al mismo tiempo, esos avances tecnológicos han traído consigo riesgos en la seguridad de las personas y de sus legítimos intereses como usuarios. El uso de los modernos medios de pago no es una excepción.

Como hemos visto en capítulos precedentes, la lista de fraudes realizados mediante los nuevos mecanismos de pago es elevada. Frente a tales prácticas, como medios de erradicación se alza el Derecho Penal, es decir, la posibilidad en general de castigar con la privación de libertad a los autores de tales delitos a través de juzgados y tribunales, además de poder solicitar un resarcimiento civil de las cuantías defraudadas a las víctimas.

No obstante algunos aspectos deben ser tenidos en cuenta a la hora de afrontar la “solución penal” cuando hablamos de proteger los derechos de los consumidores y usuarios. En primer lugar, los consumidores no están especialmente interesados en privar de libertad, una vez debidamente juzgadas, a las personas responsables de la comisión de un fraude. Les interesa sobre todo el poder recuperar su dinero defraudado (ahorro, sueldos, etc.). Por eso, la búsqueda de un tipo delictivo específico para los fraudes en medios de pago exige un tipo, no sólo razonable y justo, sino sobre todo disuasorio. Estas deben ser las notas de un tipo delictivo que se enfrente a una regulación de los fraudes en medios de pago.

Por otro lado, el recurso a la vía penal exige acudir a los tribunales, lo que para los consumidores se traduce en periodos largos de espera, incertidumbre, costes etc. Por eso, establecer un procedimiento penal adecuado y justo para los consumidores, se plantea como una necesidad insoslayable.

La regulación penal española del fraude en medios de pago: demasiada confusión

Como ya hemos tenido ocasión de comprobar en la parte primera de este Estudio, el “fraude en medios de pago”, se considera desde la perspectiva penal como un delito de estafa. No obstante, no existe un criterio único para calificar este tipo delictivo, ya que depende de varios factores y circunstancias y, por otro lado, tiene varios puntos de contacto con otros tipos delictivos.

1. Los múltiples aspectos del delito de estafa y su incidencia en medios de pago

El delito de estafa requiere la producción por el autor de un engaño con la consecuencia de una situación de error que conduce a la realización por el engañado de un acto de disposición económicamente evaluable que menoscaba el patrimonio de la víctima.

La redacción típica de la estafa propia se plasma en el art. 248.1 CP que establece que:

“Cometen estafa los que, con ánimo de lucro, utilizan engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”.

No cabe duda de que este tipo delictivo es el que se ajusta a los fraudes cometidos en medios de pago. Este engaño se entiende como maniobra que puede conducir a error al otro, pero siempre como fruto psicológico de una relación personal. Es por esto que la estafa convencional requiere un contexto personal entre los intervinientes. Los hechos más habituales de empleo fraudulento de medios de pago tienen que ver con las tarjetas de pago en sus distintas versiones. Por ello y de acuerdo con la concepción predominante del elemento típico del engaño los supuestos fundamentales que vamos a incluir en el tipo de estafa del núm. 1º del art. 248 serán los de pago presencial con tarjeta de crédito u otros instrumentos de pago electrónico, bien por el titular del instrumento jurídico de pago en determinadas condiciones, o bien el empleo del mismo por un tercero no titular.

El requisito del engaño y el debate sobre su presencia en las conductas fraudulentas sobre aparatos automáticos

Como elemento central del delito, la naturaleza que se otorgue al engaño permitirá o no la extensión del hecho punible a nuevos supuestos como los hechos fraudulentos cometidos sobre aparatos o mecanismos automáticos y otros. Debido a una concepción personalista del engaño típico de la estafa, en el ámbito de la modalidad de este delito que podemos considerar clásica del art. 248.1 CP, se incluirán todos aquellos supuestos en los que se

empleen medios de pagos electrónicos, pero que requieran la presencia física o contacto personal de las dos partes de la operación.

Por tanto, de acuerdo a esto, el comportamiento nuclear de la estafa gira en torno al engaño, a la acción fraudulenta. Ahora bien, en el ámbito de la estafa ha existido tradicionalmente el problema de no admitirse los engaños a máquinas o instrumentos automáticos.

En realidad esta problemática se presentaba de modo semejante en los países de nuestro entorno pues procedía de los nuevos hechos asociados a la emergente delincuencia informática, como es el caso de Alemania.

Casos de pagos presenciales y la incidencia de los deberes de diligencia:

Los supuestos más habituales de estafa mediante el pago con medios de pago que supongan algún tipo de operación electrónica serán de abono del producto o servicio a través de tarjetas de crédito o débito u otros recursos en algún tipo de establecimiento comercial. Para los pagos mediante la presentación de la tarjeta de crédito en establecimientos comerciales es necesario hacer dos distinciones:

a) Pagos realizados por el titular del instrumento:

Si el titular utiliza la tarjeta una vez que ha sobrepasado su límite de vigencia, ha excedido en los límites de pago admitidos para la tarjeta, o cuando la misma le ha sido anulada por la entidad emisora tratando de engañar y lograr un indebido beneficio patrimonial, puede incurrir en responsabilidad penal.

b) Pagos por terceros sin consentimiento del titular:

Los casos más frecuentes son los de utilización ilegítima de la tarjeta por un tercero sin consentimiento del titular. Entre ellos se suele incluir la utilización no consentida por un tercero para obtener alguna cantidad de dinero de una entidad financiera o para realizar el pago de productos o servicios adquiridos directamente en un estable-

cimiento comercial. De forma que quien finge ser el titular de una tarjeta en una operación presencial para lograr la entrega de ciertos bienes o la prestación de algún servicio crea una falsa apariencia de crédito con la presentación de la misma frente al comerciante o empleado.

Pese a la calificación de las tarjetas magnéticas o perforadas como llaves falsas en el art. 239 CP, resulta difícil que sea de aplicación para estos casos en los que realmente lo que sucede es un engaño sobre la titularidad de la tarjeta mediante la presentación de la misma, la firma de los comprobantes o la pulsación del número secreto que habilita para su utilización.

Además del caso más común de pago mediante tarjeta de crédito o de débito existen otros medios de pago que implican algún tipo de transmisión electrónica en la realización de la operación. Aunque menos aceptados y con un desarrollo menor, existen mecanismos como la tarjeta monedero, el pago mediante el teléfono móvil, los cheques electrónicos o el dinero electrónico, en sentido estricto.

Normalmente estos nuevos sistemas están pensados para facilitar el pago a distancia, sin que se requiera la presencia física de quien efectúa el pago y quien lo recibe. Sin embargo, como sucede con la tarjeta de crédito o de débito, es posible su empleo en una relación comercial directa y personal. En estos supuestos si se diese tal relación de intermediación y de acuerdo con los presupuestos interpretativos del elemento del engaño, la posible infracción penal se correspondería con la estafa propia del art. 248 CP.

La estafa electrónica en los pagos en redes de telecomunicación.

La posición de la jurisprudencia española sobre el problema del engaño, es negarse a admitir el engaño sobre máquinas o aparatos automáticos.

De este modo el legislador prevé un supuesto específico de estafa informática (art. 248.2 CP) en la que se castiga la manipulación de datos o sistemas informáticos para lograr una transferencia no consentida de activos patrimoniales. De forma que el art. 248.2 CP señala:

La inexistencia de una adecuada normativa de protección al consumidor en fraudes con tarjeta, obliga a acudir a los Tribunales penales

La escasa normativa española sobre contenido de contratos, prevención y delimitación de responsabilidades ante fraudes a través de medios de pago, hace que toda la "protección" que pueda de los usuarios se establezca en los tribunales penales. Ello supone demasiado tiempo e incertidumbre, ya que ni siquiera los jueces tiene claro el tipo penal a aplicar. Al consumidor no le interesa la pena impuesta al delincuente, sino el resarcimiento del daño sufrido o su prevención.

En España, toda la normativa de carácter "civil" (que se refiere al cumplimiento de los contratos y a las obligaciones entre las partes), procede de Directivas Europeas.

■ En materia de **transferencias bancarias**, existe la ley 9/1999, que fija los plazos de ejecución de las transferencias, coste, responsabilidad en caso de cumplimiento tardío, etc. No obstante, esta normativa (cuyo origen es la Directiva 97/5/CE ya comentado) no se aplica curiosamente a las transferencias cuyo origen y destino sea el territorio español, sino a las que se realizan entre España y otros países de la UE, de ahí su poca trascendencia. No obstante, la Circular 8/90 del Banco de España, en su Anexo IV, sí establece las fechas de valoración (a efectos del cómputo de intereses), dependiendo si se trata de transferencias internas (el mismo día de la orden) o externa (el segundo día hábil desde la orden).

■ En materia de **tarjetas**, no existe normativa legal, ya que se mantiene el contenido de las "Recomendaciones" europeas de los años ochenta y noventa sobre responsabilidad en el uso fraudulento de tarjetas, y que ya hemos analizado en la Parte de este estudio dedicado a la normativa Europea. Sin embargo, sí existe una buena regulación garantista en materia de pago con tarjetas en compras por Internet y devoluciones de cargos indebidos por fraude. Su origen es la Directiva 97/7 de Ventas a Distancia, y se recoge en el artículo 106 de la actual Ley General de Defensa de los Consumidores y Usuarios RDL 1/2007

■ El **proyecto de Ley sobre "servicios de pago"** (transposición de la Directiva 2007/64 que actualmente se está tramitando en el Parlamento Español) recoge en único texto todas estas cuestiones y, además, lo cual es una novedad, la extiende a toda la operativa ya se realice con otras entidades europeas o exclusivamente entre entidades españolas. Para su estudio más detallado, nos remitimos a la Parte de este estudio donde se recoge la normativa europea.

“También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiguen la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero”.

La misma pena se aplicará a los que fabricaren, introdujeran, poseyeran o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo.

2. Fraudes con tarjeta y su calificación penal

Según el Tribunal Supremo, en Acuerdo del Pleno no jurisdiccional de la Sala Segunda del 28 de junio de 2002, el art. 387 del Código Penal contiene una “cláusula de asimilación”, ya que, según el artículo 386 CP, que regula el delito de falsificación de moneda, se puede considerar moneda, además de la metálica y papel, “las tarjetas de crédito, las de débito”.

La doctrina se ha planteado si se puede considerar la manipulación de la banda magnética de este medio de pago, donde se introducen datos de otro obtenidos fraudulentamente, “fabricación de moneda falsa” a los efectos del artículo 386 CP. Ello conlleva la aplicación de una pena de prisión de 8 a 12 años, además de la responsabilidad por el delito de estafa en el que también incurrirá el autor cuando emplee la tarjeta. En caso contrario estaríamos en el supuesto de falsedad en documento mercantil, donde las penas son mucho menos graves.

Al respecto, el Pleno no jurisdiccional de la Sala Segunda, en su reunión de 28-6-2002, adoptó el siguiente Acuerdo:

“Las tarjetas de crédito o débito son medios de pago que tienen la consideración de «dinero de plástico», que el art. 387 del Código penal equipara a la moneda, por lo que la incorporación a la «banda magnética» de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el art. 386 del Código penal. En tales supuestos, dada la imposibilidad de determinación del «valor aparente» de lo falsificado, no procede la imposición de la pena de multa también prevista en el referido precepto. Asimismo, se pronuncia el Pleno favorablemente a la procedencia de que por el Tribunal competente para la resolución del recurso de casación, se acuda, a tenor de lo dispuesto en el art. 4.3 del Código penal, al Gobierno de la Nación exponiendo la conveniencia de la inclusión, en el Código penal, de un precepto específico que contemple los actos de falsificación de tarjetas, con establecimiento de las penas adecuadas para cada supuesto, en consonancia con lo previsto para esta materia por la Decisión Marco del Consejo de Ministros de la Unión Europea sobre «la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo», de 28 de mayo de 2001”.

Clases de ilícitos penales en tarjetas: no hay unanimidad

1) Fraudes en soportes físicos (cajeros automáticos, TPV, etc)

El fraude en cajeros automáticos puede realizarse tanto a través del uso de tarjetas reales, sustraídas indebidamente o utilizadas ilícitamente, como a través de tarjetas falsas. La diferencia en lo que se refiere a la calificación del ilícito puede resultar esencial.

En el caso de utilización de tarjetas reales, indebidamente apropiadas o sustraídas, no estaríamos en principio ante una manipulación informática ya que no se modifican los sistemas de control y funcionamiento del sistema. La doctrina señala que al no producirse manipulación no existe engaño por lo que se podría aplicar a este caso el artículo 248.2 relativo a la estafa. En este caso, tendríamos que referirnos más bien a una apropiación de cosa mueble.

2) Fraude en establecimientos comerciales

En estos casos el establecimiento comercial actúa como un tercero que intermedia entre el titular de la tarjeta y su emisor. Este tercero tiene una actuación decisiva, tanto en relación a la clasificación de los hechos como en la perfección del negocio jurídico, y una serie de obligaciones de control y supervisión. El caso de que el hecho se produzca a través de una tarjeta real no sería de aplicación el supuesto de estafa del 248.2 del Código Penal entre otras causas porque no se produce manipulación informática. Respecto al engaño la discusión se centra en si es el encargado del establecimiento el que lo sufre o bien es directamente el sistema informático el que no detecta la identidad falsa, última opción esta que habría que descartar por lo que si se observan correctamente los mecanismos de autoprotección sería el dependiente el engañado y si podríamos hablar en este caso de estafa.

3) Fraudes on-line, (contratación por Internet de producto o servicios, e-banking, etc.)

La aparición de la banca on line ha posibilitado nuevas formas de negocio y evidentemente ha originado también nuevas tipologías de fraude. En caso de que la numeración introducida provenga de una tarjeta real la mayoría de la jurisprudencia ha optado por aplicar el tipo básico de estafa ya que entienden que el engañado es la persona que realiza la disposición del objeto o servicio tras comprobar la autorización del sistema informático. La misma interpretación aunque con diversos matices se ha dado para los casos de fraude por internet utilizando una tarjeta falsa..

¿Cómo castigar el uso de tarjeta de crédito y número secreto sustraídos para extraer dinero de cajero automático?

La supuesta es el de extraer dinero de cajero automático utilizando una tarjeta de crédito sustraída a su legítimo propietario. ¿en qué tipo penal debe encajarse esa obtención de dinero de un tercero de forma ilícita? La apreciación como delito de robo se sustenta en que su comisión lo es con fuerza en las cosas “por el uso de llaves falsas”, ya que en el art. 239 párrafo último del Código Penal equipara éstas a las tarjetas magnéticas. Por tanto, si se sirve el autor de una tarjeta magnética que introduce en el cajero automático, teclea un número asociado a la misma y saca una cantidad de dinero, la acción descrita se comprendería en el apoderamiento de cosas muebles ajenas empleando fuerza en las cosas para acceder al lugar donde se encuentran

Sin embargo, otras apreciaciones llevan a que el supuesto planteado se recoge en determinadas resoluciones judiciales como delito de “estafa informática” según el art. 248.2 del CP, el que dispone que son reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiguen la transferencia no consentida no consentida de cualquier activo patrimonial en perjuicio de tercero. Se apoya en primer lugar esta postura en que en caso alguno concurre acceso al lugar donde se halla el dinero cuando se extrae de un cajero por el método de uso de tarjeta y número secreto sustraídos a su titular, habiendo expulsión de dinero sin acceso.

La doctrina se decanta claramente por considerar el supuesto planteado como un delito de **robo con fuerza en las cosas** y no por una estafa informática. Y ello porque ésta presenta demasiados problemas de interpretación en sus elementos que pueden violentar el principio de legalidad, ello a pesar de que el término acceso hay que interpretarlo de una forma no exclusivamente material, sino en función del resultado obtenido.

3. Phishing y Pharming Bancario: las entidades de crédito no pueden hacer recaer la responsabilidad exclusiva en sus clientes

En la mayoría de los casos de transferencias fraudulentas de fondos analizados por el Servicio de Reclamaciones del Banco de España, el problema fundamental reside en la correcta identificación del cliente y en las medidas de autenticación ofrecidas por la entidad. A pesar de que, con carácter general, las entidades de crédito cuentan con medidas de seguridad internas a efectos de prevenir y minimizar el fraude electrónico, contribuyendo a mejorar la seguridad del canal (también las advertencias realizadas a través de las propias páginas web de las entidades y el envío de comunicaciones periódicas a sus clientes son buenas medidas divulgativas des-

tinadas a concienciar al cliente), estas medidas, muy importantes en su fin, no son suficientes para eludir los riesgos que analizamos, pues las actuales sofisticaciones de los fraudes electrónicos superan las posibilidades del cliente medio, que, en general, no es un experto en seguridad informática.

Las medidas de seguridad actuales de bancos y cajas no son suficientes

En definitiva, ninguna de estas medidas por separado, ni todas ellas en su conjunto, son concluyentes a la hora de evitar las actuales vías de fraude electrónico, que atacan principalmente al usuario mediante técnicas de ingeniería social o intrusiones en los equipos y/o comunicaciones informáticos.

Evidentemente, el diseño de las medidas de seguridad entra dentro del ámbito de actuación discrecional de cada entidad; estamos ante una decisión adoptada por cada entidad al diseñar su política operativa y comercial. Así, es de sobra conocido que los sistemas de autenticación ofrecidos a los clientes de banca electrónica por la mayoría de las entidades de crédito son sistemas débiles o de un solo factor (una clave fija o aleatoria), a pesar de que la mayoría de los expertos en seguridad informática coinciden en señalar que las medidas de autenticación son más eficaces si incorporan dos factores: algo que el cliente conoce (una clave) y algo que el cliente tiene (un token, un teléfono móvil, etc.). Estos sistemas de doble factor podrían evitar la captura indebida de la firma electrónica y, por consiguiente, el fraude.

¿Dan a conocer Bancos y Cajas los riesgos a los usuarios?

En la medida en que la elección de uno u otro sistema de autenticación afecta al grado de seguridad en el que las operaciones, comunicaciones y datos de sus clientes están protegidos frente al acceso o la modificación por terceros no autorizados, entendemos —en la línea expuesta por la Comisión Europea— que resulta de gran importancia que los consumidores comprendan los riesgos de aceptar el sistema de autenticación ofrecido por la entidad con la que operan y que conozcan cuál es la mejor alternativa posible para poder prevenir un fraude. En este sentido, si bien en los contratos se informa al cliente de las condiciones para operar y de las consecuencias que le depararía un uso indebido de sus claves, no se le suele advertir del riesgo de que estas puedan ser capturadas por los ciberdelincuentes para su posterior uso con fines delictivos, ni de que, en este caso, deberá soportar los quebrantos ocasionados (incluso aunque dicha captura no se hubiera realizado como consecuencia de la falta de la diligencia que le resulta exigible en su calidad de usuario). Por otro lado, tampoco podemos olvidar que el usuario de banca electrónica puede acceder a este servicio no solo desde su equipo en su domicilio, sino también desde lugares públicos, como bibliotecas, hoteles o cibercafé, y, en muchos casos, sin necesidad de un puesto fijo gracias a las redes inalámbricas. Algu-

nas entidades dan publicidad a esta facilidad en su página web, destacando que la banca electrónica «permite realizar todo tipo de operaciones bancarias a través de Internet desde cualquier lugar en el que se encuentre y a cualquier hora».

El cliente no puede ser el único responsable

Dicho esto, puede resultar un tanto incongruente que, si la entidad no ha limitado expresamente las vías de acceso a este canal, pretenda que su cliente sea el único responsable de la falta de seguridad del equipo a través del cual se efectuó la operación presuntamente fraudulenta. Tampoco comparte el Servicio de Reclamaciones del Banco de España la conclusión a la que llegan algunas entidades (tras comprobar que no ha existido fallo alguno en sus sistemas informáticos) cuando precisan que es al cliente, en calidad de perjudicado, a quien corresponde seguir las diligencias judiciales que se instruyan como consecuencia de la denuncia interpuesta por el fraude sufrido, debiendo entretanto asumir el coste de las operaciones fraudulentas. Así, teniendo en cuenta que:

- a) Son las entidades las que han puesto en funcionamiento un nuevo canal operativo para sus clientes, cuyo uso fraudulento puede devenir en graves perjuicios para los mismos.
- b) Este uso fraudulento puede venir producido no solo por la negligencia de los clientes, sino por un desconocimiento más que comprensible de los riesgos asumidos o por la vulnerabilidad de los sistemas de autenticación utilizados.
- c) Los sistemas de autenticación son elegidos por las entidades, existiendo casos en los que otros sistemas pueden proporcionar una mayor seguridad a la hora de la correcta identificación de los clientes de banca electrónica.

La estafa electrónica en el código penal español

El delito más habitual -por cuanto engloba una amplia variedad de conductas delictivas- es la estafa informática. Regulada en el artículo 248 del Código Penal, en su apartado 1 se distingue entre los supuestos de estafa basados en técnicas de ingeniería social pura (donde se sitúa el phishing): “Cometen estafa los que, con ánimo de lucro, utilicen engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”; y los supuestos de utilización de código malicioso (malware) o de intrusión en sistemas de información recogidos en el artículo 248.2 del CP: “También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero”.

Criterios de actuación que deben aplicar bancos y cajas

No parece equitativo ni proporcionado que las entidades eludan sin más su responsabilidad, dirigiendo a sus clientes a los tribunales de justicia y haciendo recaer en los mismos la totalidad de los importes defraudados. Por ello, el Servicio de Reclamaciones del Banco de España considera que (al margen del recurso a los tribunales de justicia) la actuación de las entidades de crédito en relación con el supuesto fraude debe ser analizada teniendo en cuenta los siguientes principios de buenas prácticas bancarias:

1 De información, por el que las entidades deben asegurarse de que sus clientes:

a) En la fase precontractual, conocen la realidad y magnitud del riesgo que comporta operar a través de la Red, especialmente con el sistema de autenticación que les es ofrecido, a fin de poder comparar el mismo con otros existentes en el mercado.

b) Al suscribir el contrato, son conscientes de los compromisos que asumen.

c) Reciben la formación y el asesoramiento necesarios para operar de la manera más «segura», siguiendo así las directrices ya avanzadas, el 26 de enero de 2001, por la Comisión Europea.

2 De diligencia, por el que, advertidas del supuesto fraude, las entidades deben actuar con la diligencia que les es exigible como profesionales en la materia para gestionar la recuperación de los fondos fraudulentamente transferidos. A este respecto, las asociaciones profesionales del sector han formalizado acuerdos de colaboración para posibilitar la recuperación de estos importes.

3 De responsabilidad, por el que se entiende que la realización de estas operaciones a través de Internet es posible únicamente porque las entidades han implantado este sistema (con los mecanismos de seguridad y autenticación que han considerado convenientes) y lo han divulgado, adquiriendo por ello, según este Servicio, una responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

LA INDEFENSIÓN EN QUE QUEDA EL CLIENTE ES INJUSTA

En definitiva, no sería equitativo ni acorde con una actuación calificable de buena práctica bancaria hacer recaer automáticamente la negligencia o culpa y el consiguiente perjuicio en el cliente que sufre el fraude. En opinión del Servicio, el hacer recaer en su cliente toda la responsabilidad, así como la carga de la prueba de haber actuado correctamente —acreditando que no facilitó sus claves por haber recibido un spam con un vínculo a una página falsa de la entidad, que no operó en ningún momento desde un equipo desprotegido por no contar con un antivirus/firewall actualizado, etc.—, coloca al cliente en una situación de inferioridad y de indefensión frente a la entidad, que es la que ha ofrecido el sistema a su cliente y ha elegido los mecanismos de seguridad que ha estimado más convenientes. Por ello, se consideró su actitud contraria a los buenos usos y prácticas financieros.

4. El uso fraudulento de chips de pre pago en estafas telefónicas

La Fiscalía General del Estado estableció una serie de criterios, a través de su Consulta 3/2001, sobre la calificación jurídico-penal de la utilización, en cabinas públicas de teléfonos y móviles de pre pago de instrumentos electrónicos que imitan el funcionamiento de los legítimos monederos electrónicos cuyo objetivo es establecer una conexión telefónica; puede servir para entender el fraude cometido en este tipo de instrumentos de pago; interpretación extensible a los múltiples fraudes y estafas cometidos desde ese momento hasta la actualidad.

Los métodos o mecanismos utilizados por los defraudadores y su posible calificación jurídica

Se trata, por lo general, de un soporte de plástico al que se incorporaba un circuito integrado que, según los informes periciales elaborados al respecto y que cita la Fiscalía

consultante, consistía en un circuito formado por dos series de tres contactos que se comunicaban, mediante unos filamentos, con un chip de 11×7 mm., aproximadamente, en el que el dispositivo electrónico que incorporaba ofrecía un comportamiento idéntico al de los monederos electrónicos. Mediante un programa grabado en el chip se proporcionaban las órdenes oportunas al dispositivo del teléfono por ejemplo, validando los datos correspondientes como las claves y los códigos necesarios, así como la cantidad equivalente en pesetas disponible durante la llamada.

Dicha cantidad solía ser la máxima utilizada en las tarjetas originales (12 euros), cantidad que el programa del chip regeneraba automáticamente una vez consumida, lo que permitía una utilización prácticamente ilimitada de la misma en una o en múltiples llamadas. Estas tarjetas se fabricaban en laboratorios clandestinos, que disponían de sofisticados medios informáticos, y eran, en aquel momento, productos altamente cotizados en el mercado también clandestino que generó tanto su alquiler como su venta.

Manipulación fraudulenta de tarjeta: ¿un delito de falsedad documental?

Se planteó su posible incriminación como delito de falsedad documental. Con arreglo a la definición del artículo 26 CP, no cabe duda de que los monederos electrónicos (tarjetas de pre pago, etc) son un genuino documento a efectos penales. La tarjeta pre pago puede ser alterada en alguno de sus elementos o requisitos de carácter esencial (nº 1 del art. 390.1), con lo que se produciría una lesión de la fe y seguridad en el tráfico jurídico, ya que se pretendería disponer de un justificante documental aparentemente válido en el supuesto de que se suscitase alguna controversia sobre la validez de la tarjeta.

De manera similar, es imaginable también simular un monedero electrónico en todo o en parte, de manera que induzca a error sobre su autenticidad (nº 2 del art. 390.1). La simulación total del documento tendría lugar, por ejemplo, si se elaborase un soporte plástico de las mismas dimensiones y con los mismos datos impresos y en

El acceso a la Justicia de los Consumidores de Servicios Financieros

El reconocimiento legislativo y político, por parte de todos, de los derechos de los consumidores, en España muy notoriamente desde la Ley General de Consumidores y Usuarios de 1984 y posteriormente con una panoplia de legislación específica, incluido el sector de productos y servicios financieros, no ha conseguido garantizar la eficacia de esos derechos. Es necesario plasmar eficazmente los principios que en lo referente a los sistemas extrajudiciales de resolución de conflictos que han quedado reflejados en diversa normativa europea (Recomendación de la Comisión Europea de 4 de abril de 2001 y Recomendación 98/257/CE): Imparcialidad, transparencia, eficacia y equidad.



**CONSIGA ESTA
INTERESANTE Y AMENA
PUBLICACIÓN**

Llámenos: ADICAE
C./ Gavín, 12 local. 50001 ZARAGOZA
Tfno.: 976 390060 ■ Fax: 976 390199
email aicar.adicae@adicae.net

los mismos colores que una tarjeta original, y que externamente tuviese la misma apariencia que el documento original. Sin embargo, la conducta que se venía detectando era una burda falsificación, para la que se utilizaba un soporte de plástico u otro material rígido sin ninguna pretensión de simular una tarjeta auténtica.

Tampoco podía hablarse de falsificación material del chip, ya que la alteración en este no pretende en ningún caso engañar a otra persona mediante la producción de efectos probatorios u otro efecto jurídico que pueda estar asociado a la presentación del documento, ya que la manipulación del mismo es evidente y no pretende ser ocultada.

Un supuesto que no encajaría en la calificación de estafa

Es aplicable en parte la doctrina sentada en su día por la Consulta nº 4/93 de la Fiscalía General, que abordó el problema de la calificación jurídico-penal de las manipulaciones fraudulentas en las tarjetas multivaje de los transportes públicos urbanos. Concretamente, pese a afirmar que dichas tarjetas eran verdaderos documentos mercantiles, negó la posibilidad de subsumir el hecho analizado en el delito de falsedad de los arts. 302.º y 303 CP de 1973, porque se trataba de una falsificación incapaz de inducir a engaño en una simple inspección del documento.

No obstante lo anterior, concluía la citada Consulta que la alteración de las tarjetas multivajes anteriormente descrita podía ser constitutiva de un delito de estafa, en la medida en que el sonido producido por la tarjeta alterada al ser introducida en la máquina canceladora, indiferenciado del sonido que producen las tarjetas legítimas, estimula en quienes realizan funciones de vigilancia la errónea representación de estar utilizando una tarjeta válida, por lo que confluyen los elementos del engaño y el error que exige el tipo de la estafa, a los que se añaden el acto de disposición patrimonial, consistente en la conducta omisiva del vigilante que tolera el acceso, y el consiguiente perjuicio, consistente en el disfrute de un servicio por parte de quien no lo ha pagado.

Sin embargo, en la utilización de un chip clandestino en una terminal telefónica, por ejemplo, aunque tienen lugar el acto de disposición (prestación del servicio de llamada por parte de la compañía) y el perjuicio (no abono del precio del servicio) faltan tanto el engaño como el error, ya que no existe ninguna persona que de manera similar al vigilante del transporte pueda ser considerado sujeto pasivo de ambos.

El supuesto tipificado de estafa informática

El art. 248.2 CP, castiga a los que con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiguen la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. La conducta típica, a la vez que maneja el concepto de manipulación informática o artificio semejante, que prima facie podría tener encaje en el supuesto analizado, introduce otros elementos del tipo cuya concurrencia resulta evidente, como el ánimo de lucro, el carácter inconstituido de la prestación y el perjuicio de tercero. Sin embar-

go, no se puede decir lo mismo de la concurrencia del concepto transferencia de activo patrimonial, ya que en el supuesto analizado no se transfiere propiamente ningún bien del patrimonio de un sujeto al de otro, sino que simplemente se disfruta de un servicio de manera inmediata, de tal modo que una vez finalizada la operación y agotada la prestación del servicio no se puede decir que el patrimonio del sujeto activo se haya visto incrementado.

Fraude a través de telecomunicaciones

Otra posibilidad incriminadora de la conducta analizada es la ofrecida por el tipo del art. 255.1º ó 3º CP, que castiga al que cometiere defraudación utilizando telecomunicaciones (cuando se utiliza como tarjeta de prepago), u otro elemento o energía ajenas, valiéndose de mecanismos instalados para realizar la defraudación o empleando cualesquiera otros medios clandestinos. En este caso, la inclusión de la conducta en el tipo queda fuera de toda duda. Como muy difícilmente esta modalidad de defraudación superará las cincuenta mil pesetas, habrá de ser calificada por lo general como una falta del art. 623.4 CP, que prevé idéntica pena para las faltas de estafa informática y de defraudación de telecomunicaciones. En cualquier caso, aun sosteniendo que es posible la configuración de la conducta como una estafa informática, el tipo del art. 255 CP resultaría de aplicación preferente en virtud del principio de especialidad (regla 1ª del art. 8 CP).

Por otra parte, aquellos que fabrican y facilitan los chips manipulados a los usuarios finales deben considerarse cooperadores necesarios en la infracción. Sin embargo, la conducta consistente en la mera fabricación de estas tarjetas para su posterior uso, pero sin constancia de su utilización efectiva, no superaría el estadio de los denominados actos preparatorios impunes.

Delito de estafa en telecomunicaciones

La conducta consistente en la utilización en móviles o en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago ha de ser calificada como una infracción de defraudación de telecomunicaciones, prevista y penada en los arts. 255.1º y 3º ó 623.4 CP, en función de la cuantía defraudada.

Por su parte, la conducta de quienes fabrican los citados instrumentos, o de cualquier manera se los proporcionan o facilitan a los usuarios finales, es un supuesto de cooperación necesaria en la infracción anteriormente mencionada. Las conductas consistentes en la fabricación o tenencia de tales instrumentos, con fines de comercialización y el correspondiente ánimo de lucro, aun sin constancia de que hayan llegado a ser utilizados, pueden ser asimismo constitutivas del delito contra la propiedad industrial previsto y penado en el arts. 273.3 CP, siempre que la topografía del circuito integrado reproducido esté debidamente protegida mediante su registro, y del delito contra la propiedad intelectual contemplado en el art. 270 CP, si bien en ambos casos se exige como requisito de procedibilidad penal la denuncia del perjudicado (art. 287.1 CP).

La protección penal de los consumidores y usuarios exige cambios procesales

El olvidado principio “pro consumatore”

Por imperativo de la Constitución española, concretamente en su art. 51, los poderes públicos están obligados a garantizar la defensa de los consumidores y usuarios y a proteger, “mediante procedimientos eficaces”, la seguridad, la salud y los legítimos intereses económicos de los mismos. Además, los derechos otorgados a los ciudadanos por los artículos 24 y 25 de la Constitución, en virtud de los cuales todas las personas tienen derecho a obtener la tutela efectiva de los Jueces y Tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión, son corolario evidente de la concepción social o asistencial del Estado Democrático de Derecho, tal y como ha sido configurado por nuestra Norma Fundamental.

No hay tutela judicial efectiva para los consumidores sin mejores medios

La realidad nos demuestra que la complejidad de los procedimientos penales (y pensemos muy en particular en las complejidades técnicas de los fraudes en medios de pago, la dificultad de los medios probatorios, el problema de la distancia en la comisión del delito, etc.) puede contribuir a ver insatisfecho este derecho si no existen unos medios adecuados a la complejidad y reiteración del fraude. Esta complejidad se evidencia en el uso de complicadas técnicas tecnológicas, el carácter organizado de la delincuencia, así como su actividad en terceros países. Todo ello contribuye a enmarañar el esclarecimiento de los hechos.

La formación financiera de los juzgados: un reto para la defensa de los consumidores

En primer lugar, es imprescindible optimizar las infraestructuras humanas y técnicas de los Órganos judiciales encargados de la instrucción y enjuiciamiento de tales conductas. Por su especial complejidad en los fraudes financieros en medios electrónicos de pagos, sería fundamental la implementación asistencial técnica tanto al juez instructor, al Ministerio Fiscal y a las partes acusadoras, al fin de desentrañar y comprender correctamente el “laberinto” de estos procedimientos y su excesiva duración.

Un nuevo tipo penal concreto para los fraudes en medios de pago

En segundo lugar, sería deseable que no se demorase por más tiempo la aprobación de una nueva Ley de Enjuiciamiento Criminal, que debería incluir una perfecta sistemática de este tipo de delitos (de los que ya existe variada casuística) y no tener que subsumirlos en tipos tan generales como el de la estafas.

El problemas del auxilio judicial internacional en los delitos económicos de fraude en medios de pago

En general en los llamados “delitos económicos” y, en particular, en los fraudes financieros a través de medios de pago en nuevas tecnologías (cuya comisión se efectúa con carácter masivo y cuyo origen en la mayoría de las ocasiones tiene lugar en territorio distinto de donde se produce el resultado) las pruebas solicitadas a través del Auxilio judicial internacional (pruebas a realizar en países extranjeros) se constituyen como una de las más necesarias al fin de localizar y, en su caso, recuperar aquellas cantidades indebidamente apropiadas o estafadas que permitan satisfacer la responsabilidad civil derivada del delito, y restaurar la situación al estado existente antes de la incidencia del hecho delictivo. Es preciso citar a modo de ejemplo que en muchos caos se remiten comunicaciones a entidades bancarias con domicilio en los llamados “paraísos fiscales”, tales como Islas Bahamas y Suiza.

Resumen del anexo I de jurisprudencia contenido en la presente publicación

Contiene sentencias sobre:

- **Tarjetas**

- Responsabilidad y carga de la prueba
- Falsificación de tarjetas y el fraude
- Envios y retiradas irregulares de tarjetas
- Incorporación de cláusulas abusivas a los contratos

- **Transferencias y recibos**

- Errores en la ejecución
- Adeudos de recibos no domiciliados

- **Cheques**

- **Phishing**

Parte 4

Las malas prácticas y condiciones abusivas de bancos y cajas con relación a los medios de pago



Hemos visto que, pese a la profusión de normas, no existe hasta el momento, un texto normativo completo y eficaz para los derechos de los consumidores que, en materia de medios de pago, regule jurídicamente de forma unitaria esta materia. Existen disposiciones dispersas incluidas dentro de diversas normas jurídicas (Ley 9/1999 sobre transferencias internacionales, Ley 7/1996 de Ordenación del Comercio Minorista; Ley 7/1998, de Condiciones Generales de la Contratación; Ley 19/1985, Cambiaria y del Cheque...) En el siguiente apartado vamos a analizar cómo se plasma esa carencia de sustantividad normativa propia en la realidad.

¿Dispone el consumidor de mecanismos y vías eficaces para resolver sus conflictos en materia de medios de pago? ¿Hay un control efectivo de las cláusulas que aparecen en los contratos de medios de pago? Al margen de los tribunales, cuya actuación y sentencias, analizaremos en el capítulo siguiente, vamos a centrarnos en las “soluciones” que ofrece el Banco de España, máximo organismo supervisor de las entidades de crédito en nuestro país.

La ausencia de regulación jurídica unido al efecto no vinculante de los informes/resoluciones del Servicio de Reclamaciones del Banco de España son los principales motivos de frustración de los derechos de los usuarios, ante la situación preponderante de las entidades. El Código de Buena Conducta es insuficiente para regular el sector. Además, como se ha puesto de manifiesto, resulta ineficaz, ya que las entidades ante la arbitrariedad de su aplicación, prescinden (o lo interpretan a su criterio incluyendo limitaciones) de Código tanto en el clausulado de sus contratos como en la práctica bancaria ordinaria. Posiblemente el futuro proyecto de ley de servicios de pago mejore esta situación en nuestro país. A nivel Europeo la Directiva 2007/64/CE sobre servicios de pago podría suponer un avance en la defensa de los derechos de los usuarios de servicios de medios de pago, ya que va más allá de las meras “recomendaciones” y buenas “voluntades” que sugiere el fracaso Código.

No obstante, las Resoluciones del Banco de España analizadas podrían servir como base sobre el que en un futuro, en el proyecto de ley de servicios de pago, se articule un cuerpo normativo específico concreto, donde se regulen jurídicamente esas “malas prácticas bancarias” y establezca un marco de mínimos en el que toda cláusula contractual contraria a los criterios del Banco de España fuese declarada nula.

Análisis de las malas prácticas de las entidades en medios de pago: fraudes que se repiten año tras año

El consumidor se enfrenta continuamente a situaciones abusivas cometidas por bancos y cajas, en una posición de total inferioridad. Ante esto, ninguna institución ni poder público ofrece una protección eficaz y los órganos supervisores carecen de la potestad necesaria para sancionar y poner freno a estas conductas.

Existen un gran número de conductas que podemos catalogar como malas prácticas o prácticas abusivas cometidas año tras año por las entidades, conductas que no podemos analizar como una lista cerrada ya que su tipología aumenta conforme lo hacen las nuevas tecnologías y las nuevas posibilidades de operatividad para el consumidor, muy especialmente en el caso de los medios de pago que nos ocupa.

1. El banco de España, el órgano supervisor de las entidades, no ofrece una protección eficaz al consumidor

Todas las malas prácticas y abusos al usuario que vamos a exponer en este capítulo han sido sistematizadas a partir de las Resoluciones que dicta el Servicio de Reclamaciones del Banco de España. Constituye una buena muestra del “catálogo” de irregularidades que año tras año cometen las entidades de crédito con relación a medios de pago (pero también a otros muchos contratos y servicios financieros con consumidores) Por eso, consideramos que es un buen “material” para establecer una regulación garantista y protectora de los derechos de los consumidores. Pero si hay que sacar otra conclusión, es que **los mecanismos de protección extrajudicial para los consumidores deben mejorar**. Vamos a ver, antes de analizar el contenido de las reclamaciones, cómo funciona este Servicio.

En relación al ámbito de los medios de pago, como respecto de otros contratos y servicios financieros, **el Banco de España tiene atribuida competencia para tutelar las relaciones de transparencia entre las entidades de crédito y los usuarios**. Esta competencia la ejerce a través del Servicio de Reclamaciones del Banco de España creado en 1987. Este Servicio de Reclamaciones tiene a su cargo la tramitación de las quejas o reclamaciones y consultas. Es el encargado de recibir los escritos, reclamar las actuaciones relacionadas con éstos, instruir los expedientes, cumplimentar y dar traslado de las actuaciones, cursar todas las comunicaciones y, en general, los actos de trámite en los expedientes, así como redactar, los Informes de conclusión de los expedientes.

Las entidades ignoran las resoluciones del Banco de España

Pero estos Informes carecen de efectos vinculantes para las entidades, ya que suponen una opinión del Servi-

cio, o dicho de otro modo, el consumidor que obtiene un Informe favorable a sus derechos sólo puede “confiar” a que la entidad se acoja “voluntariamente” a lo dictaminado por el Servicio de Reclamaciones, algo que hará voluntariamente y sin ningún tipo de repercusión si se opone a ello.

En la práctica las entidades pueden obviar el informe remitido por el Banco de España sin que conlleve ninguna consecuencia.

En efecto la normativa ha establecido que tales Informes carecen de la naturaleza jurídica de actos administrativos, por tanto, no puede ser objeto de recurso. Así en la resolución de 1 de marzo de 1996 señala textualmente que “no engendra derechos ni obligaciones para los interesados como tal dictamen, no tiene el carácter de resolución ni constituye un acto de trámite a efectos del artículo 107.1 de la citada Ley 30/1992, por lo que no cabe recurso contra el mismo”. Como consecuencia, no tiene eficacia vinculante, y además, no puede fijar una indemnización por daños y perjuicios: “No es competencia de los Comisionados para la defensa del cliente de servicios financieros decidir ni pronunciarse sobre los daños y perjuicios que eventualmente haya podido ocasionar a los usuarios de los servicios financieros la actuación, incluso sancionable, de las entidades sometidas a supervisión, ni facilitar valoración económica alguna”. (Art. 5.3 del Rgto.)

Las malas prácticas recogidas anualmente por el Banco de España, pueden servir como base para la regulación

Los Informes o Resoluciones del Servicio de Reclamaciones del Banco de España pueden servir como base sobre la que en un futuro se articule un cuerpo normativo específico concreto, donde se regule jurídicamente las malas prácticas bancarias recogidas en sus Memorias, y en particular las que se refieren a las actuaciones de bancos y cajas en medios de pago que defraudan los derechos de los consumidores.

ESQUEMA-INDICE MALAS PRÁCTICAS:

- En tarjetas
- En cheques
- En domiciliaciones de recibos
- En transferencias

2. Tarjetas bancarias: criterios del Banco de España sobre abusos de Bancos y Cajas con los usuarios

Robo, sustracción, uso fraudulento, duplicidad y clonación de tarjetas de débito o crédito

Después del aviso de sustracción dado por el titular, es la entidad la que ha de hacerse responsable de cualquier disposición que se haya podido llevar a cabo pues, aunque demuestre que ha puesto todos los medios a su alcance para evitarlas, se estima que existe una responsabilidad objetiva en la entidad que es la que crea el sistema y lo implanta.

Frente a ello, el cliente al que se hace entrega de una tarjeta de crédito o débito asume la responsabilidad de su custodia.

Por ello se estima que **la responsabilidad por las disposiciones efectuadas antes del aviso de sustracción recae normalmente sobre el titular, salvo que concurren circunstancias particulares** que, en su caso, habrían de ser consideradas por los tribunales de justicia.

Desde la perspectiva de las buenas prácticas y usos bancarios, tiene especial importancia el Código de Buena Conducta, que en su norma 12 dispone un límite de responsabilidad, a modo de autoseguro, para el caso de que sea el titular -por tratarse de disposiciones anteriores al aviso de pérdida o sustracción- quien deba asumir los cargos fraudulentos, estableciendo que **"el titular no soportará aquellas pérdidas que excedan del límite de 150 euros, salvo que hubiese actuado de forma fraudulenta, a sabiendas o con negligencia grave** o no haya observado las cláusulas 6 (a) y (c) de este Código", relativas estas últimas a la necesidad de observar la debida diligencia en la custodia de la tarjeta y de su número secreto y a la obligación de avisar de la pérdida, robo o copia de la misma a la entidad emisora, sin dilación alguna. Esta norma se ha recogido expresamente en la Directiva 2007/64/CE, y en el Proyecto de Ley, por el cual se incorporará dicha Directiva a nuestro ordenamiento.

Las entidades tienen la obligación, por tanto, de recoger en los contratos de tarjetas un límite a la responsabilidad del titular acorde con lo estipulado en el Código.

Hay que recordar que el límite de 150 €, siempre que sea recogido en los términos expuestos en el citado Código, constituye una garantía para los usuarios de este medio de pago, habida cuenta que, en principio, los titulares están sujetos al deber de diligente conservación o custodia de la tarjeta, por lo que deberían ser responsables de las operaciones efectuadas con la misma. Claro, que atendiendo al caso concreto habría situaciones en las que sería la entidad la que debería hacerse cargo totalmente.

La no aplicación por las entidades del citado límite, solo puede justificarse si se acredita la existencia de negligencia por parte del titular de la tarjeta en su custodia o conservación, si bien corresponde a los tribunales de justicia valorar esta circunstancia. En ningún caso se admite la presunción de falta de diligencia en la custodia del PIN, por el hecho de que la utilización fraudulenta de la tarjeta se haya llevado a cabo con el tecléo correcto del número de identificación personal.

Cuando se producen incidencias de esta naturaleza, robos, sustracciones, falsificaciones o cualquier uso irregular de medios de pago, las entidades deben utilizar los medios a su alcance para conseguir el soporte documental de las operaciones, -tickets de compra o tiras de fondo de los cajeros automáticos, pudiendo comprobar así la realización de las operaciones controvertidas, retrocediéndolas inmediatamente cuando concurren irregularidades que así lo exijan.

Las entidades deben poner a disposición del titular todos los medios necesarios a fin de que pueda hacer efectiva la comunicación de robo o sustracción

Respecto a este punto, y haciendo de nuevo referencia a la Directiva 2007/64/CE, hay que hacer especial hincapié en la obligatoriedad para la entidad emisora de la tarjeta de poner a disposición del titular todos los medios necesarios a fin de que haga efectiva esta comunicación. Esta medida resulta razonable, ya que el hecho de que no notifique esta circunstancia conlleva gravosas consecuencias para el usuario. Entre estas medidas que debe adoptar la entidad, merece la pena destacar la puesta a disposición de sus clientes de una línea de teléfono gratuita.

Cuando se realizan transacciones en las que se cuestiona la autenticidad de las firmas, salvo aquellos casos en los que la falsificación sea evidente, serán los tribunales de justicia, los únicos que a través de la oportuna intervención pericial podrán determinar la falsedad cuestionada.

En caso de Duplicidad y Clonación si la propia documentación aportada al expediente no acredita la existencia de estos hechos, nuevamente el consumidor queda a expensas de los tribunales de justicia que serán los que se pronuncien sobre esta cuestión, úni-

cos con atribuciones para determinar lo realmente sucedido y, por tanto, resolver definitivamente la cuestión planteada.

Límite temporal de aviso

El SRBE considera que el establecimiento en el contrato de un límite temporal de aviso (desde que se produjo la pérdida, robo, hurto o extravío de la tarjeta), para notificar la pérdida de su posesión, solo puede ser admisible cuando redunde en un beneficio para los titulares de tarjetas. Por el contrario, no puede considerarse una buena práctica bancaria que la entidad proceda a la aplicación automática de este límite temporal para enervar la aplicación del autoseguro previsto en el contrato, ya que habría que analizar en cada caso concreto si concurren otras circunstancias que permitan concluir que ha habido una actuación poco diligente por parte del cliente en la comunicación a la entidad de la pérdida o sustracción de la tarjeta.

En cualquier caso, deberán ser los tribunales de justicia, y no las entidades de crédito como interesadas directas, los que declaren la diligencia de los titulares de tarjetas.

Cargo indebido o fraudulento en el caso de venta a distancia

De conformidad con lo dispuesto en el art. 46 de la Ley de Ordenación del Comercio Minorista-LOCM (actual artículo 106 del del RDLeg 1/2007, Ley de Consumidores y Usuarios), en el caso de que el importe de una compra, o el precio de la prestación de un servicio haya sido cargado de manera indebida o fraudulenta al titular de una tarjeta de pago, utilizando su número, el titular de ésta puede exigir la inmediata anulación del cargo, debiendo efectuarse a la mayor brevedad posible las correspondientes anotaciones de adeudo y rebono en las cuentas del proveedor y del titular, respectivamente.

Algún autor preconiza la aplicación analógica del art. 43. 2 de la LOCM, de manera que en el supuesto de que el vendedor no realice el abono en el plazo de 30 días, el consumidor acreedor de la cantidad cargada indebidamente podrá reclamar que se le pague el doble de la suma adeudada; aunque puede ponerse en cuestión la existencia de identidad de razón en ambos supuestos, puesto que en éste supuesto que nos ocupa el proveedor sí habrá dispuesto los bienes de consumo o prestado el servicio.

El ámbito de aplicación de esta norma no está restringido a las tarjetas de pago, haciéndose extensiva a las tarjetas de crédito o débito ya tanto a las bancarias como a las comerciales.

El contrato de tarjeta: oscuro y con trampas... cuando se entrega

El contrato de tarjeta, según lo dispuesto en la norma sexta de la Circular del Banco de España 8/1990,

sobre transparencia de las operaciones y protección de la clientela, **deberá estar debidamente firmado por las partes, determinando sus derechos y obligaciones.**

Asimismo, las entidades tienen la obligación de conservarlo en la forma legalmente prevista.

Para los contratos de tarjeta formalizados con anterioridad a 1991 (fecha en que el Código de Buena Con-

Pagos realizados a través de Internet: todavía inseguros

El criterio es que el consumidor devuelva el recibo y el banco le reintegre el cobro

El libre consentimiento prestado al uso del medio de pago elegido para la transacción comercial, debe tener los mismos efectos jurídicos que la firma de la factura expedida por el proveedor, que constituye una prueba escrita de la prestación de consentimiento.

Si el cliente negara la existencia de la transacción comercial, la entidad, ante tal argumento y con la diligencia exigible en estos casos, debería iniciar la retrocesión del apunte controvertido, hasta que reciba la acreditación documental de la existencia de la operación comercial y del consentimiento prestado por el titular de la tarjeta, incluyendo la comunicación del número de dicha tarjeta, sistema habitualmente utilizado en Internet para el uso de dicho medio de pago. La entidad está obligada, como mera intermediaria en este tipo de operaciones, al cumplimiento del reglamento del sistema de tarjetas correspondiente, en especial al plazo que se señale para poder reclamar la devolución de los cargos provenientes del pago con tarjetas de compras de bienes.

Cuando se produzca controversia sobre la realización de operaciones, las entidades han de estar en condiciones de justificar la realidad de las que pretenden adeudar a sus clientes, aportando el justificante de la transacción que corresponda, uniendo el necesario respaldo contractual en aquellos casos que así se precise, remitiendo copia de los registros informáticos que reflejan la transacción cuestionada, acreditando corresponder la numeración de la tarjeta a la asignada al interesado y figurando la operación terminada normalmente. Si no es así, y además se aporta por el titular de la tarjeta una evidencia del carácter fraudulento o indebido del cargo, es indudable que no sería correcto por parte de la entidad adeudar o mantener en cuenta de su cliente las disposiciones cuestionadas.

ducta fue trasladado por las asociaciones profesionales del sector a sus afiliadas), que no recojan en su condicionado todas las prescripciones de las normas anteriores –en especial, el límite de 150 euros de responsabilidad del titular-, las entidades deberán, en cualquiera de las renovaciones que temporalmente suelen efectuarse, aprovechar la circunstancia para adaptar el clausulado de los contratos a la normativa enunciada. Esta adaptación, en definitiva, redundará en beneficio de la transparencia que, en todo caso, debe presidir las relaciones entre las entidades de crédito y sus clientes.

Lo anteriormente expuesto no es suficiente para asegurar la protección del consumidor que debido a las características de los contratos, muchas veces con cláusulas no del todo claras, el reducido tamaño de la letra, la complejidad del lenguaje utilizado y la falta de información o información distorsionada dada en las entidades, apenas puede conocer cuales son sus derechos y obligaciones en el uso de estos productos.

El límite de disposición en las tarjetas de crédito ¿se respeta?

Respecto al límite de crédito pactado, la concesión de operaciones por encima del mismo, es una decisión que se considera enmarcada dentro de la política de riesgos de la entidad, si bien hay que tener especial precaución

con los intereses y comisiones que el consumidor debe soportar por hacer uso de estas.

La entidad debería informar al titular de la tarjeta de cuál es este límite además de los gastos que genera la disposición de crédito y el mantenimiento de la tarjeta.

Si se excediera el límite máximo de disposición previsto en el contrato de tarjeta y la misma fuera objeto de pérdida, robo o sustracción, pretender cobrar del titular de la misma un importe superior al estipulado como límite de crédito merecería un pronunciamiento desfavorable del SRBE, por contravenir dicha actuación lo pactado y ser contrario a lo que demandan las buenas prácticas y usos bancarios.

No puede olvidarse que el límite de disposición establecido para las tarjetas opera, además, como un límite de seguridad para el titular de las mismas, debiendo la entidad asumir los riesgos correspondientes cuando autoriza una ampliación del mismo.

Retraso en la comunicación de los adeudos por parte de la entidad

La demora excesiva e injustificada en comunicar los adeudos en cuenta, dados los medios informáticos y tecnológicos existentes hoy día, suponen una falta de diligencia por parte de las entidades que, además, re-

Cancelación y bloqueo unilateral de las tarjetas: una práctica habitual

En este punto, nos hallamos ante una operación basada esencialmente en la confianza entre la entidad de crédito y el cliente y que, normalmente, suele presentar un plazo de duración indefinido, si bien esto último dependerá de lo que se establezca en el contrato de emisión.

A estos efectos, la disposición adicional primera de la Ley 26/1984, introducida por Ley 7/1998, de Condiciones Generales de la Contratación, admite que se puedan modificar unilateralmente, en el ámbito de los servicios financieros, las condiciones de un contrato de duración indeterminada, siempre que el prestador de servicios financieros esté obligado a informar al consumidor con antelación razonable y éste tenga la facultad de resolver el contrato. También podría la entidad de crédito emisora de la tarjeta, en su caso, rescindir el contrato unilateralmente, sin previo aviso en el supuesto de razón válida, a condición de que informe de ello inmediatamente al contratante.

Requisitos para que una entidad pueda cancelar unilateralmente una tarjeta

Las entidades deben cumplir una serie de obligaciones específicas en aquellos casos en los que decidan cancelar unilateralmente una tarjeta:

En primer lugar, la decisión de resolver debería estar fundada en causas objetivas -como ha manifestado el Tribunal Supremo en sentencia de 15 de noviembre de 1994, RJ 1994/84888.

En segundo lugar debe comunicarse previamente sus intenciones al titular de la tarjeta, a fin de evitar que sufra perjuicios adicionales a los que, en todo caso, le originaría la anulación de la misma.

Finalmente, es acorde con las buenas prácticas bancarias restituir al cliente la parte de la cuota periódica de mantenimiento de la tarjeta ya satisfecha, en proporción al plazo en que la misma no será disfrutada por aquél.

Aún en el caso de que las razones comerciales o de política de riesgos justifiquen el bloqueo de la tarjeta, siempre e ineludiblemente la entidad debe comunicar su decisión previamente al interesado, evitando la situación de indefensión que lo contrario puede provocarle.

sulta contraria al principio de claridad y transparencia que debería presidir las relaciones entidad/cliente, considerándose, por tanto, este tipo de actuaciones contrarias a las buenas prácticas y usos bancarios.

Los descubiertos en cuentas corrientes

En los contratos de crédito en cuenta corriente, que no sean una cuenta de tarjeta de crédito, **la entidad de crédito está obligada a informar por escrito al consumidor, antes de la celebración del contrato o en el mismo momento y de forma individualizada, del tipo de interés efectivo anual, así como de los gastos, posibles modificaciones y procedimiento para resolver el contrato.**(Ley 7/1995, de 23 de marzo, artículo 19.1 y Circular del Banco de España 8/1990, de 7 de septiembre, norma sexta, apartado 11).

En el caso de descubiertos en cuenta aceptados tácitamente por la entidad de crédito, el consumidor deberá ser informado del tipo de interés efectivo anual aplicado y de sus modificaciones. (Ley 7/1995, de 23 de marzo, artículo 19.3).

Por otra parte, se limita el tipo de interés aplicable a los descubiertos en cuenta corriente de consumidores. Así, el artículo 19.4 de la Ley 7/1995, de 23 de marzo, de Crédito al Consumo, establece que en ningún caso se podrán aplicar a los créditos que se concedan en forma de descubiertos en cuentas corrientes un tipo de interés que de lugar a una Tasa Anual Equivalente superior a 2,5 veces el interés legal del dinero.

Las entidades de crédito están obligadas a publicar de forma separada, en el tablón de anuncios existente en sus oficinas, el tipo de interés aplicable a los descubiertos en cuenta corriente de consumidores.

El criterio que mantiene el Servicio de Reclamaciones para calcular la Tasa Anual Equivalente del descubierto en cuenta corriente es que para el cálculo de la limitación cuantitativa que impone la Ley de Crédito al Consumo, deben tenerse en cuenta todos los conceptos, incluidas las comisiones, que por el descubierto se cobre al consumidor, sobre la base de que el coste total de un crédito incluye todos los gastos y cargas que el consumidor vaya a pagar por el mismo.

En definitiva, las comisiones por descubierto en cuenta corriente de consumidores han de ser consideradas al momento del cálculo de la TAE resultante para las mismas y ésta, así calculada, no puede exceder de la cuantía que representa 2,5 veces el importe del interés legal del dinero.

Disposiciones no justificadas y errores por parte de las entidades

Las entidades emisoras de tarjetas tienen que mantener un sistema que permita llevar registros suficientemente detallados, en los que quede constancia de las operaciones realizadas y que puedan permitir, en su caso, la rectificación de los errores que se hubieran producido.

Como se establece en el Código de Buena Conducta sobre la protección de los consumidores en materia de

medios de pago, en su artículo 15:

"Si el tenedor de la tarjeta niega que su tarjeta y, en su caso, el NIP u otro código se han usado para efectuar una transacción o alega que dicha transacción se ha realizado de forma incorrecta, el emisor deberá mostrar, mediante extracto de un registro interno, que la operación fue fielmente registrada y anotada en las cuentas y no se vio afectada por ninguna avería o deficiencia. Los registros correctos de semejantes transacciones tanto anteriores como posteriores deberán constituir la prueba a primera vista de que el sistema funciona debidamente".

En consecuencia, las entidades deberán aportar copia de los registros informáticos que reflejen la transacción cuestionada, en particular copia de la tira de fondo del cajero, incluyendo las operaciones anteriores y posteriores, y documento acreditativo del cuadro del citado cajero en la fecha en la que se realizó la disposición, con el objetivo de poder comprobar que la numeración de la tarjeta utilizada se corresponde con la asignada al interesado y que la operación se ejecutó correctamente. Este listado opera, conforme establece el Código anteriormente citado, como auténtico y único registro para validar la corrección o no del reintegro.

Cuando el cajero automático no esté operativo o no facilite, por motivos circunstanciales, resguardo de la operación, estamos ante incidencias ocasionales en la operativa bancaria que, en sí mismas, no pueden valorarse como merecedoras de crítica, salvo que presenten una grave reiteración o se den circunstancias de una actuación negligente en su solución.

¿Qué pasa si hay retención de la tarjeta por el cajero?

Cuando la tarjeta resulte capturada en un cajero, apareciendo la leyenda: "Retenida por orden de Central. Tarjeta en lista negra. No devolver tarjeta. Inutilicela" u otras similares, la entidad propietaria del cajero, se limita a ejecutar la orden de retención dictada por la Central; retención que, por otra parte, se basa en razones de seguridad dirigidas a proteger, con carácter general, los intereses de los titulares de las tarjetas que resulten retenidas y de los emisores de las mismas, sin que, por ello, pueda devolverse la tarjeta al interesado, aún cuando éste acredite – mediante documento idóneo– que es el titular de la misma, debiendo recabar de la entidad emisora de la tarjeta las explicaciones oportunas sobre lo ocurrido y las razones que han motivado que la entidad propietaria del cajero ejecutase la correspondiente orden de retención.

En el mismo sentido, cuando la retención se produce como consecuencia de haberse excedido el tiempo de espera programado en el cajero automático, no obedeciendo a un acto unilateralmente decidido por la entidad sin comunicación al interesado. En tales circunstancias conviene adoptar medidas de seguridad complementarias, para evitar que la tarjeta quede a merced de posibles usos fraudulentos, debiendo prevalecer, en este caso, la seguridad sobre cualquier otra consideración.

Otra cuestión sería la retención de la tarjeta por problemas de funcionamiento operativo del cajero, como puede ser una caída de tensión de la línea o un corte del fluido eléctrico, hecho fortuito, siempre que sea aislado y no merecedor de un pronunciamiento desfavorable por parte del SRBE. Ahora bien, aún en el supuesto de que la entidad no sea responsable, en este caso, de la interrupción de un servicio, ello no es impedimento para que se adopten las medidas necesarias para limitar los perjuicios que se deriven de las incidencias surgidas en la utilización de las tarjetas.

No obstante lo anterior, si los errores fueran reiterados o existiera demora en su subsanación, supondrían una falta de diligencia contraria a las buenas prácticas y usos bancarios.

Emisión, retirada y envío de tarjetas sin solicitud previa o por medios que no aseguran su recepción

Cuando no se acredite la previa solicitud del cliente (exceptuando la remisión de plásticos por renovación del documento), el envío discrecional de tarjetas basado en criterios comerciales se considerará contrario a las buenas prácticas bancarias. Además, en aquellos casos en que las entidades realicen campañas promocionales, vía telefónica, con el objetivo de «colocar» determinadas tarjetas entre sus clientes, sería deseable que no remitieran el plástico mientras no estuviera convenientemente firmado el correspondiente contrato, evitando así malentendidos respecto a la voluntad de sus clientes de contratar el producto ofertado. En este sentido, la existencia de un documento contractual, en el que se establezcan los términos y condiciones de utilización de los medios de pago, se considera elemental para la defensa de la claridad, transparencia y justo equilibrio de las prestaciones, y así se recoge en la cláusula primera del Código de Buena Conducta de la Banca Europea, con respecto a los sistemas de pago mediante tarjeta, y en la CBE n.º 8/1990, que, en su norma 6.ª, establece la obligatoriedad de entrega del documento contractual en la emisión de medios de pago vinculados a las cuentas corrientes o de ahorro.

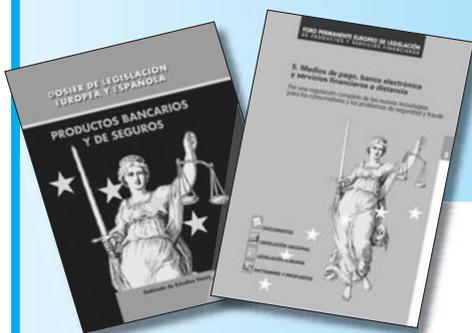
La cláusula octava del citado Código de Buena Conducta establece que el emisor de la tarjeta no deberá entregar una tarjeta no solicitada a un cliente, salvo cuando la tarjeta sustituya a otra que ya poseía el cliente.

El SRBE considera mala práctica bancaria la remisión por correo ordinario de documentos de trascendencia económica, como lo son las tarjetas de crédito y el número secreto de la misma, ya que es conocido que, en general, este sistema no garantiza ni la certeza de la recepción del documento por parte del destinatario, ni la constancia documental de que la propia entrega se ha efectuado. Dicho esto, y teniendo en cuenta que el momento de la recepción de la tarjeta es básico para conocer desde cuándo el titular tiene a su cargo el deber de su custodia, así como el de denuncia, en caso de verse desposeído de la misma, las entidades deben adoptar las medidas oportunas para, en definitiva, obtener certeza de que la tarjeta se entregó al titular o persona autorizada, mediante el correspondiente acuse de recibo o cualquier otra forma válida.

Disposiciones fraudulentas con tarjeta de débito, cuyo importe excede el saldo de la cuenta asociada

El saldo depositado en la cuenta asociada a una tarjeta de débito constituye un límite natural a las disposiciones que con aquella se puedan realizar, salvo que se acredite expresamente que se pactó la posibilidad de que el cliente realizase pagos en descubrimiento hasta un determinado importe. Por tanto, de no existir ningún pacto, las entidades deberán rechazar tales pagos, asumiendo su importe, en caso contrario, si se acredita que han sido realizados fraudulentamente.

En algunos de los expedientes del SRBE, las entidades adeudaron, en las cuentas de sus clientes, disposiciones (supuestamente fraudulentas) efectuadas con tarjetas de débito, a pesar de que su importe superaba el saldo que presentaban sus cuentas vinculadas y de que no se acreditó que existieran pactos previos que les permitieran admitir disposiciones por encima de sus saldos acreedores.



Medios de pago, banca electrónica y servicios financieros a distancia

Por una legislación completa de las nuevas tecnologías para los consumidores y los problemas de seguridad y fraude

CONSIGA TODAS ESTAS
INTERESANTES Y
AMENAS
PUBLICACIONES

Llámenos: ADICAE

C./ Gavín, 12 local. 50001 ZARAGOZA

Tfno.: 976 390060 ■ Fax: 976 390199

email aicar.adicae@adicae.net

3. Cheques: malas prácticas en su operativa

Forma y lugar de pago del cheque

Durante el plazo de presentación, tan sólo puede denegarse su pago si hay denuncia por robo o extravío, siempre que exista saldo en la cuenta.

Las normas que regulan el lugar de pago de los cheques (básicamente los artículos 106, nº 4 y 107 de la Ley 19/1985, de 16 de julio (BOE del 19) Cambiaria y del Cheque) establecen que, a falta de indicación especial, el lugar designado en el cheque junto al nombre del librado se reputará lugar de pago del mismo, por lo que ninguna sucursal distinta de la indicada en el mismo tiene la obligación legal de pagar en efectivo el cheque.

Hay que tener en cuenta que **pagar un cheque por ventanilla en oficina distinta a aquella en la que el firmante tiene cuenta abierta implica un riesgo, al no poder comprobar que su firma coincide con la del titular de la cuenta**, medida de seguridad necesaria para evitar pagos de documentos a un tenedor ilegítimo o que no hayan sido regularmente emitidos.

El pago en efectivo de los cheques

No existe norma que limite los pagos en efectivo, por lo que las entidades vendrán obligadas, salvo que aleguen la existencia de una causa objetiva que así lo impida, a realizar tales pagos el mismo día en que sean requeridas para ello.

No obstante, en aquellos casos en los que las entidades presenten alguna dificultad para hacer frente al pago de cantidades que por su elevado importe excedan del encaje que en ese momento tenga la oficina, no se considera mala práctica bancaria la demora de unas horas o incluso un día en atender el pago. A estos efectos sería recomendable que los clientes avisaran previamente de su intención de retirar cantidades elevadas en efectivo.

Pago de documentos falsificados

La cuestión tiene tratamiento específico en los artículos 154, 155 y 156 de la Ley Cambiaria y del Cheque.

El SRBE no puede pronunciarse sobre supuestas falsificaciones; sobre si las partes actuaron con culpa o negligencia en la custodia y libramiento de los talones, o en el seguimiento de las operaciones de su cuenta; o si las entidades no actuaron de forma diligente al efectuar el pago de los documentos falsificados.

Si la entidad se negara a devolver el documento presuntamente manipulado al cliente, alegando la comisión de un presunto delito, la retención llevada a cabo carecería de justificación, al privar al tenedor del documento de ejercer las acciones que, en su caso, pudiera considerar oportunas para conseguir el cobro del documento.

La solicitud de Identificación de los presentadores del cheque

Solicitar la identificación al tenedor de un cheque, con independencia de cómo se encuentre emitido y de cual sea su importe, es una medida que promueve la seguridad del tráfico cambiario y mercantil y que, por lo tanto, de emplearse, debe considerarse beneficiosa. En todo caso **el RD 1393/1993 establece la obligatoriedad de exigir la presentación del NIF de la persona que presente al cobro un cheque librado por una entidad de crédito**, siempre que su abono no se realice en una cuenta bancaria, así como cuando el librador del cheque sea persona distinta al presentador, y su importe exceda los 3.005 euros.

En este sentido, la propia Ley Cambiaria y del Cheque, en su artículo 140 advierte que el banco puede exigir que el cheque se le entregue con el "recibí" del tenedor, señalando, a estos efectos, que el librado podrá exigir al pago del cheque que éste le sea entregado con el recibí del portador.

Los procedimientos de envío deben ser seguros

Es necesario utilizar un procedimiento de envío que ofrezca seguridad y que permita acreditar la recepción por el destinatario, no pudiendo olvidar que se trata de documentos de importancia trascendental como es el original de un documento cambiario.

Además, una vez producido el extravío se deben arbitrar medios para conseguir que los clientes procedan al cobro de los efectos, extendiéndose un certificado de extravío ajustado al modelo normalizado establecido en el Anejo V de la Instrucción SNCE A/08/526.

Las entidades son responsables de las actuaciones de terceros (valijas, courier, etc.), tanto más si anuncian como reclamo publicitario su funcionamiento operativo sin sucursales, deben poner los medios para que ninguna incidencia sea achacable a los tipos de organización tradicionales. Si ellas establecen el sistema, responden de su funcionamiento.

4. Domiciliación bancaria

Adeudo de recibos domiciliados

Es imprescindible que exista autorización previa de carácter genérico por parte del titular de la cuenta, para que todas las órdenes de adeudo de iguales características puedan ser imputadas en cuenta sin preaviso. Se podría considerar la existencia de una orden tácita cuando se han recibido reiterados adeudos en la cuenta por domiciliación, sin que el ordenante se manifieste en contra.

En este sentido, **las entidades deben guardar constancia documental de la orden de domiciliación**. La entidad presentadora deberá remitir la misma a solicitud de la entidad domiciliataria, dentro de los plazos.

Por ello, en los casos en que no es posible el cargo automático por no existir orden de domiciliación expresa ni autorización genérica, se recomienda que la entidad receptora realice gestiones para procurar el cobro antes de proceder a la devolución.

Igualmente, es imprescindible, según su propia definición, que el recibo cuente con un código cuenta cliente C.C.C. Ahora bien, la carencia de este requisito es subsanable, de forma que, aunque exista un error en el mismo, dicho error puede no ser determinante para la devolución.

No obstante se considera buena práctica bancaria que las entidades pongan todos los medios a su alcance para tratar de subsanar las deficiencias observadas en la gestión de pago, antes de proceder a su devolución, en cumplimiento de la normativa específica aplicable.

Los clientes deben contar en su cuenta con la oportuna provisión de fondos para atender el pago de los recibos domiciliados. No es preceptivo que la entidad de crédito requiera al cliente para que efectúe la correspondiente provisión, aunque dicha actuación sería considerada como una buena práctica bancaria. En caso de no contar con ella, se produciría la devolución.

Adeudo de recibos no domiciliados

Existe la práctica muy extendida entre las entidades de proceder al adeudo indiscriminado de los recibos que cuenten con un código correcto de cuenta del cliente. Dicha práctica ha sido implantada por las propias entidades en aras a una mayor agilidad operativa, lo cual, en definitiva, redonda sobre todo en su propio beneficio.

En aquellos casos en que los clientes discrepen con los cargos no autorizados, la entidad librada debe asumir en última instancia los perjuicios correspondientes y esto es así aún en el supuesto de que el plazo interbancario de devolución haya transcurrido, y que, por consiguiente, resulte imposible la devolución del recibo. No obstante, hay que puntualizar que, en ocasiones, por el transcurso de un periodo de tiempo manifiestamente dilatado desde que se produce el adeudo hasta que el cliente manifiesta su oposición, se podría apreciar una aceptación tácita del cargo.

Remisión de información al consumidor

El elemento esencial para conocer la información que se ha de facilitar a los clientes que soportan el adeudo en su cuenta es el procedimiento elegido por el emisor de los recibos para la presentación al cobro de los mismos, de tal modo que, cuando el procedimiento utilizado es el identificado con el código "02" —que es el usado en los supuestos reclamados—, las entidades deben limitarse a transmitir los datos que han recibido, ajustándose con ello a las buenas prácticas bancarias.

En cuanto a la justificación de los pagos realizados se entiende que el deudor justifica suficientemente el pago mediante el correspondiente apunte bancario, si bien, en el ca-

so de considerar que no fuera suficiente, habrá de dirigirse a la entidad emisora de los recibos, que es la que puede decidir el procedimiento de presentación de los mismos.

Orden de devolución a la entidad

Aún en el caso de adeudo contando con domiciliación previa, la normativa reguladora prevé la posibilidad de que el cliente de una orden de devolución.

Estas normas distinguen entre un **plazo normal de devolución, fijado en 9 días hábiles, cualquiera que sea el motivo, y un plazo excepcional de devolución de 30 días naturales, para el caso de que el cliente rechazara posteriormente el adeudo en su cuenta**, aduciendo error en la domiciliación o disconformidad en el importe, siempre que este sea igual o inferior al establecido para estos casos en el "Convenio sobre intercambio de Adeudos por domiciliaciones".

Por su parte, el citado convenio establece el importe de los recibos que se pueden devolver en el plazo de 30 días, igual o inferior a 3.000 €. En ambos supuestos el cómputo de los plazos se inicia a partir de la fecha de intercambio de la presentación original de los recibos. Fuera de estos plazos, la entidad domiciliataria puede intentar que la entidad presentadora admita la devolución, pero dicha devolución siempre va a estar condicionada a la gestión que realice la entidad presentadora con el cliente ordenante.

La posesión por parte del titular de la cuenta de un justificante de pago de un recibo hace que pueda presumirse que el mismo ha sido atendido con cargo a la cuenta, por ello resulta aconsejable que al dar la orden de devolución se entregue el original, de modo que pueda preservarse la seguridad del tráfico mercantil, siendo deseable que se explique este hecho a los clientes para que no transcurran los plazos de devolución.

Cuando se produce una devolución, las entidades deben justificar la causa de la misma y su diligencia en las gestiones realizadas. Por ello, deben guardar los oportunos justificantes que acrediten su diligencia en la gestión y su falta de responsabilidad en la eventual devolución de dicho envío. La falta de justificación de las causas que motivan los retrasos padecidos en las devoluciones de los documentos vulneraría las buenas prácticas bancarias.

En cuanto a la orden de devolución, es conveniente que las entidades guarden constancia documental de las mismas.

El horario de pago impuesto por las entidades

En este caso, se trata del pago de recibos, fundamentalmente de suministros y comunidades de propietarios, cuyos obligados al pago, clientes o no de las entidades de crédito, prefieren pagar los mismos en efectivo por ventanilla. **No existe disposición legal alguna que establezca un determinado horario como obligatorio para que las entidades de crédito admitan ingresos y**

realicen pagos a sus clientes, o a terceros por cuenta de sus clientes, y las entidades justifican la imposición de limitaciones horarias basándose en motivos organizativos y de optimización de la operativa bancaria, ofreciendo vías alternativas —domiciliaciones, cajeros automáticos, banca telefónica o Internet— para realizar las mismas operaciones, con un horario mucho más amplio.

Por tanto, mientras estas limitaciones horarias tengan la intención expuesta, se trata de decisiones de las entidades incardinadas en su política de funcionamiento operativo interno y, por tanto, en su esfera discrecional.

5. Transferencias bancarias

Discrepancias en los apuntes en cuenta

Las entidades están obligadas a acreditar de un modo fehaciente el consentimiento de sus clientes a cada apunte anotado en su cuenta. Además, en el supuesto de transferencias efectuadas con el exterior, durante los cinco días hábiles desde la fecha de aceptación de la orden o la recepción de los fondos un documento con la liquidación de dicha transferencia.

Igualmente, desde el punto de vista de las prácticas bancarias, estas entidades tienen la obligación de ofrecer toda la información solicitada por sus clientes con la mayor brevedad posible por cualquier tipo de operación que estos les encarguen.

El SRBE, siguiendo la doctrina Jurisprudencial del Tribunal Supremo, reconoce la obligación de conservación por parte de las entidades (tanto en beneficio de sus clientes como en su propio interés) toda aquella documentación relativa al nacimiento, modificación y extinción de los derechos y de las obligaciones que les incumben, al menos durante el período en que, a tenor de las normas sobre prescripción (15 años para las acciones personales, en virtud del artículo 1964 del Código Civil o el plazo previsto por las normas forales), puedan resultarles conveniente promover el ejercicio de los primeros, o sea posible que les llegue a ser exigido el cumplimiento de las segundas (sentencias n.º 277/2006, de 24 de marzo, y n.º 1046/2001, de 14 noviembre).

Sin perjuicio de lo anterior, habrá que estar al caso concreto. De este modo se establece también un deber de diligencia para los clientes, los cuales habrán de comunicar el incidente a su entidad dentro de un plazo de tiempo razonable.

El SRBE se ha manifestado sobre distintas cuestiones relacionadas con actuaciones de las entidades que han dado lugar a adeudos o abonos no deseados por sus clientes. En algunos casos **por abonos en cuenta distinta de la ordenada, por error de la entidad o por aplicación no autorizada de compensación de posiciones deudoras del mismo cliente en la entidad, que en todos los casos si no existe rectificación inmediata por parte de ésta, es considerada constitutiva de una mala práctica bancaria.**

La entidad no siempre puede hacer una retrocesión del cargo

En el caso de errores por abonos indebidos de transferencias, el criterio del Servicio es que una vez asentada la transferencia en la cuenta destinataria, incluso aunque quede demostrado que el abono es erróneo, se considera que la entidad receptora no está facultada para su retrocesión en virtud de simples instrucciones del ordenante de la transferencia, ya que las cantidades abonadas en cuenta no pueden ser retrotraídas si no media el oportuno consentimiento del beneficiario o la preceptiva orden o mandato legal. Como excepción a este criterio, nos encontramos con la retrocesión de aquellos abonos erróneos en cuentas de clientes, por fallos informáticos o administrativos, que una vez comunicados y justificados debidamente al cliente pueden ser retrocedidos, ya que es criterio igualmente mantenido por el Servicio que la comisión de un error no puede dar lugar a la obtención de un lucro injustificado.

Falta de diligencia en la realización de transferencias

Las faltas de diligencia en el cumplimiento del mandato recibido de su cliente es objeto de pronunciamiento contrario a las buenas prácticas bancarias, entendiendo el SRBE que la misma es impropia de entidades que profesionalmente se dedican a estos cometidos.

En el caso de gestión de transferencias, en el que intervienen dos o más entidades, en calidad de ordenante, corresponsal y beneficiario, adquiere especial importancia el hecho de que las entidades realicen todas las gestiones necesarias para el buen fin de la operación, o en su caso averiguar las causas de las posibles incidencias que hayan podido dar lugar a que ésta no se haya realizado de acuerdo con las instrucciones recibidas.

La falta de información y documentación en perjuicio del consumidor

La falta de información o información deficiente, siempre es constitutiva de una mala práctica bancaria, debiendo esforzarse las entidades en todo momento en que primen los principios de claridad y transparencia en las relaciones con sus clientes. En especial **las entidades deben asegurarse de que sus clientes conocen el coste de la operación que van a ordenar, valorándose positivamente el hecho de que en aquellos casos en los que el cliente manifiesta su deseo de transferir fondos de su cuenta, se le informe de los medios alternativos de que dispone y de los distintos costes que suponen los mismos.**

En algunos expedientes del SRBE las entidades efectuaron transferencias desde las cuentas de sus clientes, sin haber podido acreditar que contaban con su previa autorización, lo que denotó que, o bien las órdenes preceptivas no fueron convenientemente formalizadas, o que la entidad no custodió debidamente la documentación. Y todo ello con independencia del criterio del Ser-

vicio de Reclamaciones relativo a la aceptación tácita de los apuntes en cuenta sobre los que sus titulares no han manifestado ninguna disconformidad en un plazo razonable. El transcurso del tiempo, de conformidad con lo expuesto en los criterios generales, no exime a las entidades de justificar documentalmente que realizaron las transferencias cuestionadas siguiendo las instrucciones de sus clientes.

Falta de diligencia en la reclamación de transferencias fraudulentas realizadas a través de internet

Las asociaciones profesionales del sector crediticio, durante el año 2005, hicieron público entre sus asociados el procedimiento que se había de seguir para la reclamación de transferencias de fondos efectuadas fraudulentamente por Internet, como respuesta al incremento detectado de actuaciones delictivas.

Generalmente, las transferencias fraudulentas por Internet se llevan a cabo mediante suplantación de la personalidad de los clientes de banca electrónica, previa obtención por distintos procedimientos de sus datos y claves de identificación.

En este sentido, las asociaciones consideraron que una rápida reacción, tanto del cliente como de las entidades ordenante y beneficiaria de la transferencia, permitiría recuperar los fondos transferidos fraudulentamente, fijando para ello el siguiente procedimiento operativo:

- **Entre la entidad ordenante y su cliente:** Si la incidencia la detecta la entidad, debe confirmar con su cliente la existencia de fraude. En cualquier caso, indicará al cliente la necesidad de que presente denuncia por estos hechos y aporte copia de la misma.

- **Entre las entidades implicadas** (ordenante y beneficiaria):

- La entidad ordenante solicitará telefónicamente a la entidad beneficiaria (aun sin haber recibido todavía la copia de la denuncia) la retención del importe transferido.

- La entidad beneficiaria, si no hubiera abonado todavía la transferencia, la dejará en situación de «pendiente».

- La entidad ordenante deberá ratificar su petición, durante los dos días hábiles siguientes, por fax o correo electrónico. Si no lo hiciera, la entidad beneficiaria podría levantar la retención.

- La entidad beneficiaria tendrá un plazo de tres días desde esta ratificación, para devolver la transferencia, por su importe total o por la parte no dispuesta (si no hubiera fondos suficientes).

- Entre la entidad beneficiaria y su cliente, cuando este reclame la reposición de los fondos devueltos: La entidad beneficiaria reclamará a la en-

tidad ordenante ese importe y, una vez devuelto, lo consignará en el juzgado, donde se tendrán que personar la entidad ordenante o su cliente, como perjudicados. La entidad, sobre la base de la buena fe y transparencia informativa, tiene con sus clientes un deber de información que exige, entre otras cosas:

- Darles a conocer los sistemas que, en cada caso, existen para llevar a cabo una operación.

- Alertarles de las consecuencias económicas de utilizar un sistema u otro.

- Facilitarles el detalle final de la liquidación practicada.

Principios de buenas prácticas que deberían observar las entidades

- De información, por el que las entidades deben asegurarse de que sus clientes:

a) En la fase precontractual, conocen la realidad y magnitud del riesgo que comporta operar a través de la Red, especialmente con el sistema de autenticación que les es ofrecido, a fin de poder comparar el mismo con otros existentes en el mercado.

b) Al suscribir el contrato, son conscientes de los compromisos que asumen.

c) Reciben la formación y el asesoramiento necesarios para operar de la manera más «segura», siguiendo así las **directrices** ya avanzadas, el 26 de enero de 2001, por la **Comisión Europea**.

- **De diligencia**, por el que, advertidas del supuesto fraude, las entidades deben actuar con la diligencia que les es exigible como profesionales en la materia para gestionar la recuperación de los fondos fraudulentamente transferidos. A este respecto, las asociaciones profesionales del sector han formalizado acuerdos de colaboración para posibilitar la recuperación de estos importes.

- **De responsabilidad**, por el que se entiende que la realización de estas operaciones a través de Internet es posible únicamente porque las entidades han implantado este sistema (con los mecanismos de seguridad y autenticación que han considerado convenientes) y lo han divulgado, adquiriendo por ello una responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

El hacer recaer en su cliente toda la responsabilidad, así como la carga de la prueba de haber actuado correctamente —acreditando que no facilitó sus claves por haber recibido un spam con un vínculo a una página falsa de la entidad, que no operó en ningún momento desde un equipo desprotegido por

Traslación al cliente de transferencias fraudulentas realizadas a través de internet es injusto

El problema fundamental en los medios de pago reside en la correcta identificación del cliente y en las medidas de autenticación ofrecidas por la entidad. A pesar de que, con carácter general, las entidades de crédito cuentan con medidas de seguridad internas muy eficaces y acertadas a efectos de prevenir y minimizar el fraude electrónico, contribuyendo sin duda a mejorar la seguridad del canal, estas medidas no son suficientes para eludir los riesgos que analizamos, pues las actuales sofisticaciones de los fraudes electrónicos superan las posibilidades del cliente medio, que, en general, no es un experto en seguridad informática. Ninguna de estas medidas por separado, ni todas ellas en su conjunto, son concluyentes a la hora de evitar las actuales vías de fraude electrónico, que atacan principalmente al usuario mediante técnicas de ingeniería social o intrusiones en los equipos y/o comunicaciones informáticos.

La seguridad que ofrecen bancos y cajas en operaciones por internet es notoriamente mejorable

Los **sistemas de autenticación** ofrecidos a los clientes de banca electrónica por la mayoría de las entidades de crédito son **sistemas débiles o de un solo factor** (una clave fija o aleatoria), a pesar de que la mayoría de los expertos en seguridad informática coinciden en señalar que las medidas de autenticación son más eficaces si incorporan dos factores: algo que el cliente conoce (una clave) y algo que el cliente tiene (un token, un teléfono móvil, etc.). Estos sistemas de doble factor podrían evitar la captura indebida de la firma electrónica y, por consiguiente, el fraude.

En la medida en que la elección de uno u otro sistema de autenticación afecta al grado de seguridad en el que las operaciones, comunicaciones y datos de sus clientes están protegidos frente al acceso o la modificación por terceros no autorizados, resulta de gran importancia que los consumidores comprendan los riesgos de aceptar el sistema de autenticación ofrecido por la entidad con la que operan y que conozcan cuál es la mejor alternativa posible para poder prevenir un fraude.

En este sentido, **si bien en los contratos se informa al cliente de las condiciones para operar y de las consecuencias que le depararía un uso indebido de sus claves, no se le suele advertir del riesgo de que estas puedan ser capturadas por los ciberdelincuentes para su posterior uso con fines delictivos**, ni de que, en este caso, deberá soportar los quebrantos ocasionados (incluso aunque dicha captura no se hubiera realizado como consecuencia de la falta de la diligencia que le resulta exigible en su calidad de usuario).

El acceso desde otros sistemas operativos es un riesgo que no se advierte

Por otro lado, tampoco podemos olvidar que **el usuario de banca electrónica puede acceder a este servicio no solo desde su equipo en su domicilio, sino también desde lugares públicos**, como bibliotecas, hoteles o cibercafés, y, en muchos casos, sin necesidad de un puesto fijo gracias a las redes inalámbricas. Algunas entidades dan publicidad a esta facilidad en su página Web, destacando que **la banca electrónica «permite realizar todo tipo de operaciones bancarias a través de Internet desde cualquier lugar en el que se encuentre y a cualquier hora»**. Dicho esto, puede resultar un tanto incongruente que, si la entidad no ha limitado expresamente las vías de acceso a este canal, pretenda que su cliente sea el único responsable de la falta de seguridad del equipo a través del cual se efectuó la operación presuntamente fraudulenta.

Cargar la responsabilidad en el cliente es injusto

Algunas entidades (tras comprobar que no ha existido fallo en sus sistemas informáticos) precisan que es al cliente, como perjudicado, a quien corresponde seguir las diligencias judiciales, debiendo entretanto asumir el coste de las operaciones fraudulentas. Con esto se manifiesta en desacuerdo el Banco de España.

a) Son las **entidades las que han puesto en funcionamiento un nuevo canal operativo** para sus clientes, cuyo uso fraudulento puede devenir en graves perjuicios para los mismos.

b) Este uso fraudulento puede venir producido no solo por la negligencia de los clientes, sino por un **desconocimiento más que comprensible de los riesgos asumidos o por la vulnerabilidad de los sistemas** de autenticación utilizados.

c) Los **sistemas de autenticación son elegidos por las entidades**, existiendo casos en los que otros sistemas pueden proporcionar una mayor seguridad a la hora de la correcta identificación de los clientes de banca electrónica.

No parece equitativo ni proporcionado que las entidades eludan sin más su responsabilidad, dirigiendo a sus clientes a los tribunales de justicia y haciendo recaer en los mismos la totalidad de los importes defraudados.

no contar con un antivirus/firewall actualizado, etc.—, **coloca al cliente en una situación de inferioridad y de indefensión** frente a la entidad, que es la que ha ofrecido el sistema a su cliente y ha elegido los mecanismos de seguridad que ha estimado más convenientes. Por ello, se considera su actitud contraria a los buenos usos y prácticas financieros.

Falta de diligencia en la tramitación de transferencias

Las transferencias se tramitan de acuerdo con las normas reguladoras del funcionamiento del Sistema Nacional de Compensación Electrónica (que definen los aspectos técnicos y operativos aplicables entre las entidades adheridas) y en función de las instrucciones del ordenante.

Existen distintas modalidades para tramitar las transferencias. Entre ellas cabe distinguir las que se ejecutan con abono automático mediante código cuenta cliente (CCC) y aquellas otras en las que prima, sobre otras especificaciones, el nombre del beneficiario de la cuenta.

La elección de uno u otro sistema resulta esencial a efectos de determinar el procedimiento que ha de seguirse y las responsabilidades de las entidades intervinientes. En particular, del contenido de la normativa se deduce que:

- En las transferencias emitidas para abono automático mediante CCC se requiere que este código sea técnicamente correcto y figure completo (la inclusión del nombre del beneficiario titular es opcional y, en caso de figurar, se tratará como información adicional), siendo responsable la entidad ordenante de cualquier incidencia que pueda producirse como consecuencia del abono en la cuenta indicada por el CCC enviado. Las transferencias ordinarias tramitadas por esta vía no podrán exceder de 15.000 euros.

- En las otras, es obligatorio que la entidad ordenante o emisora incluya siempre el nombre del beneficiario en el campo correspondiente (considerándose los datos relativos a dígitos de control y número de cuenta, del código cuenta cliente, como complemento de la información facilitada en el campo de nombre del beneficiario). En estos casos, la entidad destinataria o beneficiaria será responsable si el abono no se efectúa al beneficiario indicado en el campo de nombre de la transferencia recibida.

Al tramitar las órdenes de transferencias de sus clientes, las entidades están obligadas a asegurar su buen fin, no limitándose a ejecutar una orden por un determinado sistema si este no es el más apropiado para la custodia de los intereses de sus clientes y la seguridad del tráfico mercantil.

Actuación incorrecta en relación con las órdenes dadas

Dentro de las modalidades de operaciones que implican un desplazamiento de fondos entre entidades de crédito, cabe diferenciar, por la entidad que recibe la orden, entre lo que son las transferencias en sentido propio (que constituyen una orden que se da a la entidad depositaria de los fondos y consistente en transferir los fondos a otra cuenta distinta, ya sea en la propia entidad o en otra distinta), y las órdenes dadas a la entidad destinataria de los fondos, que pueden ser de dos modalidades (órdenes de traspaso de efectivo y aportaciones de fondos).

Estas dos últimas son operaciones que permiten el traspaso de fondos entre dos cuentas bancarias con el mismo titular, situadas en dos entidades distintas. Otras diferencias son:

- Aportaciones de fondos: se utilizan para operaciones de menos de 3.000 euros y solo se puede hacer una operación en el mes natural. Este sistema ofrece la posibilidad de englobar varios traspasos periódicos en una única autorización.

- Traspaso de efectivo: se utilizan para operaciones de hasta 150.000 euros, sin que tenga ningún límite mínimo. Hasta 6.000 euros, estos traspasos son más cómodos para el ordenante, porque solo hay que firmar una autorización genérica. Si se superan los 6.000 euros por operación, entonces el ordenante tiene que firmar un documento específico para cada traspaso.

En estas modalidades de movimiento de dinero, la comisión que pueda existir la cobra la entidad a la que se ordena la operación, es decir, la de la cuenta de destino, que es la que gestiona el proceso.

Si el error es del cliente de la entidad ordenante emisora, entonces la citada normativa interbancaria específica que «...la entidad destinataria o beneficiaria de la operación deberá solicitar la autorización de su cliente para poder anular la operación y, en el caso de recibir la autorización, procederá a su anulación, siempre y cuando exista saldo suficiente, enviando el importe de la transferencia a la entidad ordenante emisora dentro de los cinco días hábiles del Sistema Nacional de Liquidación siguientes a la recepción de la solicitud. La entidad destinataria o beneficiaria será responsable del archivo de la autorización emitida por su cliente beneficiario de la orden, en los plazos establecidos por la Ley».

Malas prácticas bancarias más habituales en medios de pago. Resumen

- *Otorgar plena responsabilidad al titular de la tarjeta bancaria de la buena custodia de la misma; eximiéndose la entidad de toda responsabilidad en los casos de extracción fraudulenta con empleo del número PIN de la tarjeta.*
- *El establecimiento de un límite temporal de aviso para notificar la pérdida de posesión de las tarjetas a no ser que redunde en beneficio del titular.*
- *El contrato de tarjeta deberá estar debidamente firmado por las partes, determinado sus derechos y obligaciones; de lo contrario las entidades incurrirán en mala práctica.*
- *La demora excesiva e injustificada en comunicar los adeudos en cuenta suponen una falta de diligencia por parte de las entidades.*
- *El envío de tarjetas no acreditado previa solicitud del cliente se considerará contrario a las buenas prácticas bancarias.*
- *No exigir la presentación del NIF de la persona que presenta al cobro un cheque librado se considera mala práctica.*
- *Las entidades están obligadas a acreditar de un modo fehaciente el consentimiento de sus clientes a cada apunte anotado en cuenta; una actuación contraria se considera mala práctica.*
- *Abonos en cuenta distinta de la ordenada, por error de la entidad o por aplicación no autorizada de compensación de posiciones deudoras del mismo cliente en la entidad que no sean inmediatamente rectificadas por la entidad constituyen una mala práctica bancaria.*
- *La falta de información o información deficiente siempre es constitutivo de mala práctica.*
- *El hacer recaer en el cliente toda la responsabilidad así como la carga de la prueba de haber actuado correctamente en las operaciones realizadas en Internet constituye una mala práctica bancaria.*

Cláusulas abusivas en los contratos de medios de pago: abundantes y sin control previo

Cuando hablamos de Cláusulas abusivas hablamos de condiciones impuestas en los contratos por bancos y cajas de ahorros a los consumidores que perjudican sus derechos. En el negocio bancario se emplean contratos uniformes cuyo contenido está previamente establecido a través de unas condiciones generales prácticamente imposibles de modificar por exigencias particulares de los clientes, los cuales contratan “obligados” en condiciones unilateralmente impuestas por la entidad financiera: los contratos el consumidor “o lo toma o los deja”. Por tanto, esta forma de contratar puede producir un riesgo en los intereses económicos de los consumidores. Por lo que para evitar el establecimiento de cláusulas abusivas en este tipo de contratos, “contratos de adhesión”, se limita la libertad contractual por el principio de buena fe, que prohíbe la imposición de este tipo de cláusulas.

El problema que se plantea respecto a este tipo de cláusulas gira en torno a la determinación del criterio que hay que aplicar para declarar la validez o nulidad de una condición contractual. Existe una Teoría que se desarrolló inicialmente en Estados Unidos, y que aunque no de un modo expreso, sí aparece reflejada tanto en la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993 sobre Cláusulas Abusivas en los contratos celebrados con consumidores, como en la norma española de transposición (Ley 7/1998, sobre condiciones generales de la contratación). Se trata de la “Doctrina de las expectativas razonables de los adherentes”.

Esta Doctrina afirma que lo que todo consumidor acepta cuando contrata con un empresario (entidad financiera) es el objeto o servicio que adquiere, su precio, el ti-

po de contrato y cualquier otra cuestión específicamente negociada o que aparezca recogida en la publicidad de la entidad. Esta información, junto con otra serie de circunstancias relevantes, habrá formado unas expectativas en el cliente sobre la forma en la que se va a desarrollar la relación contractual. Pues bien, en la medida en que dichas expectativas sean razonables, es decir, que estén fundadas en la conducta del empresario, en disposiciones legales o en los usos y/o la buena fe, habrán de ser satisfechas. Por tanto, todas las cláusulas que impidan su satisfacción, serán nulas.

Se ha procedido a analizar una serie de entidades financieras y distintos medios de pago emitidos por las mismas, con el fin de detectar las posibles cláusulas abusivas contenidas en los contratos y efectuar su denuncia para que sean eliminadas de los mismos.

El estudio se ha realizado sobre 39 contratos, pertenecientes a 20 entidades financieras. Los contratos analizados sobre medios de pago vienen referidos a tarjetas, tanto de débito como de crédito, incluida la posibilidad de función de monedero electrónico, banca electrónica y pagos por móvil. Las entidades a que pertenecen los contratos estudiados son: IBERCAJA, CAJA LABORAL POPULAR, LA CAIXA, CAIXA CATALUÑA, BANCO SANTANDER-CENTRAL-HISPANO, CAJA INMACULADA, BBVA, CAJA VITAL KUTXA, BARCLAYS, MBNA ESPAÑA, CITIBANK, CAJA ESPAÑA, BANCO CAIXA GERAL, CAJA DUERO, CAJA RURAL DEL SUR, BANESTO, CAJASOL, CAIXA GALICIA, OPENBANK y CAJA RURAL DE EXTREMADURA.

Las cláusulas abusivas abundan en los contratos de tarjeta

A) EXENCIÓN DE RESPONSABILIDAD DE LA ENTIDAD

Los contratos ni siquiera incluyen el límite de responsabilidad de 150 euros

Una cláusula común en estos contratos es la que hace responsable al Titular de la tarjeta sin limitación alguna en los casos de “extravío o sustracción de la tarjeta” antes de la comunicación a la Entidad de tal circunstancia.

El usuario tal y como se prevé en la Recomendación y en la Directiva europea sobre medios de pago soportará las pérdidas derivadas de las operaciones de pago no autorizadas resultantes de la utilización de su tarjeta extraviada o sustraída, hasta un máximo de 150 €. Una vez comunicada la incidencia. Salvo en los supuestos de uso fraudulento por su titular; éste, una vez comunicada la incidencia, no soportará consecuencia económica alguna.

No obstante, lo expuesto con anterioridad, el emisor de la tarjeta será responsable, incluso con anterioridad a la notificación, cuando no hubiese puesto en todo momento a disposición de su cliente todos los medios adecuados para que este hubiese podido notificarle a la mayor brevedad posible el extravío o sustracción de la misma.

El usuario siempre pierde

Así mismo, se observa en los contratos sobre tarjetas que llevan incorporado la función de monedero electrónico, que el límite de los 150 €, en los casos de sustracción o extravío, no opera, ya que se considera equivalente a la pérdida de dinero efectivo, siendo indistinto que haya habido comunicación o no a la Entidad.

De nuevo, con fundamento en la Directiva europea, así como en el Proyecto de Ley de Servicios de Pago (art. 33.1), **soportará las pérdidas derivadas de las operaciones de pago no autorizadas resultantes de la utilización de su tarjeta extraviada o sustraída, hasta un máximo de 150 €, anteriores a la comunicación de la incidencia.**

Si hay fraude "paga" el cliente

En los contratos estudiados, podemos observar que siempre se hace referencia a la utilización del sistema con clave secreta para el usuario, lo que proporciona un cierto índice de seguridad. Pero, **aunque existan estipulados en el contrato sistemas de garantía para el usuario, lo cierto es que se estipulan cláusulas perjudiciales para el mismo cuando se produce un uso fraudulento de la clave secreta, exonerándose la Entidad de toda responsabilidad.**

En este sentido conviene precisar que la única causa que justifica la ausencia total de responsabilidad opera únicamente para el caso en el que debido a circunstancias excepcionales e imprevisibles totalmente fuera de su control, sus consecuencias hubiesen sido inevitables a pesar de todos los esfuerzos en sentido contrario, o cuando le sean aplicables otras obligaciones legales.

B) EXENCIÓN DE RESPONSABILIDAD POR MAL FUNCIONAMIENTO

Bancos y Cajas no quieren hacerse cargo de los defectos del cajero automático

Otra cláusula habitual que observamos en los distintos contratos analizados sobre tarjetas, es aquella por la que la Entidad se exime de responsabilidad ante incidencias técnicas en los cajeros automáticos.

Consideramos que dicha cláusula atenta contra los derechos reconocidos a los usuarios en la Ley General para la Defensa de los Consumidores y Usuarios, porque **los cajeros automáticos son propiedad de la entidad financiera, y por ello deben responder de los perjuicios que se causen al usuario por el mal funcionamiento del servicio.**

Al margen de todo esto, esta cláusula es contraria al equilibrio de las contraprestaciones; siendo responsable frente al cliente de la correcta ejecución de la operación.

Cláusula que exonera a la Entidad de toda responsabilidad en casos de interferencias, desconexión, avería en la red, etc.

Consideramos que este tipo de cláusulas son abusivas, desde el momento que la Entidad declina toda responsabilidad incluido el caso que el problema venga ocasionado por los equipos del banco o por sus técnicos. No deben incluirse en este tipo de contratos una liberación absoluta de la responsabilidad de la Entidad y hacer cargar con todos los perjuicios que se puedan ocasionar al consumidor. Al menos debería estipularse una carga de la prueba para la Entidad, de que nada ha tenido que ver con la circunstancia acaecida.

Una cláusula habitual en estos contratos es aquella por la que la Entidad se exonera de toda responsabilidad por el uso fraudulento del sistema por parte de un tercero. Independientemente de la responsabilidad penal en la que pueda incurrir el tercero que se infiltra en el sistema, la Entidad no puede exonerarse de forma automática de toda responsabilidad, ya que en atención a lo establecido en la Ley de Protección de datos, puede tener una responsabilidad administrativa, desde el momento que permite el acceso a un tercero en su sistema.

Además de la existencia de claves secretas, se hace necesario para operar a través de estos sistemas, la existencia de páginas seguras (https) por parte de la Entidad y la utilización de la Firma electrónica por el usuario a través de un ordenador seguro con sistemas antivirus.

C) FACULTADES EXORBITANTES EN FAVOR DE LA ENTIDAD

Pueden cambiar las condiciones cuando quieran

Asimismo, se observan en casi todos los contratos sobre tarjetas, ya sean éstas de crédito o débito, la existencia de una serie de facultades para la Entidad tendentes a la modificación unilateral de las condiciones pactadas. Así, por ejemplo, es habitual la cláusula que le permite a la Entidad la cancelación de la tarjeta durante el plazo de vigencia de la misma, por lo que se produce una resolución unilateral y anticipada del contrato, que resulta contraria al ordenamiento jurídico y sobre la que el Banco de España se ha pronunciado diciendo que no es equilibrada, sobre todo cuando no existe una comunicación previa y no se dan unas razones del porqué de dicha actuación.

La cláusula por la que la Entidad queda facultada para compensar los saldos entre las distintas cuentas en las que aparezca el Titular de la tarjeta, sin notificación previa y cuando se da el caso de la existencia de otros titulares en esas cuentas que no aparezcan en la cuenta asociada a la tarjeta.

D) OTRAS

¿Consultar operaciones o realizarlas?

Para sistematizar las distintas cláusulas abusivas detectadas en estos contratos, debemos hacer previamente una distinción entre si la actuación que realizamos a través de la banca a distancia es meramente informativa, o bien el acceso lo realizamos para efectuar operaciones. La distinción no es baladí, pues aunque las cláusulas abusivas afectan indistintamente al consumidor, tanto si accede a nivel informativo como a nivel operativo, las consecuencias son distintas. Así, cuando se accede a través de la banca a distancia para obtener información sobre las cuentas, fondos, acciones, etc, y se produce un uso fraudulento del sistema, se pueden producir unos perjuicios para el consumidor sobre todo lo relacionado con la protección de datos; mientras que si el uso fraudulento se produce a nivel operativo (transacciones financieras), puede ocasionar unos perjuicios también contra el patrimonio del usuario. Para evitar el uso fraudulento en las operaciones de banca a distancia, se hace necesario contar con Firma electrónica y sistemas seguros de validación de la identidad del usuario.

LOS CONTRATOS DE BANCA ELECTRÓNICA TAMBIÉN IMPONEN CONDICIONES ABUSIVAS

Con carácter general debemos empezar diciendo que, a día de hoy, existe poca regulación legal sobre el sistema llamado de banca electrónica, y la escasa regulación existente viene dada por normas de bajo rango. Es verdad, que cada vez va siendo mayor el número de usuarios que se va incorporando a este sistema para efectuar transacciones financieras, y es por ello, que tanto la Unión Europea como el Derecho interno, se han ido preocupando cada vez más de regular este sector. Así, destacamos en España como principales normas con rango de Ley que afectan al tráfico mercantil a través de internet: el Código Penal, la Ley General para la Defensa de los Consumidores y Usuarios y la Ley de Firma Electrónica. A pesar de ello, **sigue existiendo gran desconfianza en la mayoría de los usuarios a la hora de realizar transacciones financieras a través del sistema de Banca electrónica, que son producto de la inseguridad y del desconocimiento de este medio.**

No obstante lo manifestado, resulta obvio la existencia, cada vez mayor, de los llamados contratos de Banca a distancia. Y no es menos cierto, que en dichos contratos hemos descubierto la existencia de cláusulas que perjudican al consumidor, dejándolo en clara desventaja con la Entidad.

Parte 5

Problemas en medios de pago y ausencia de procedimientos de resolución rápidos y eficaces: una exigencia para los derechos de los consumidores



Una de las reivindicaciones clásicas de los consumidores y sus organizaciones es la de crear sistemas para solucionar conflictos entre empresas y usuarios que sean rápidas y eficaces. Para los consumidores, acudir a la vía judicial para resolver sus problemas resulta largo, costoso y de incierto resultado. Es evidente que el derecho procesal y los tribunales no se han adecuado a estas exigencias.

En el ámbito de los fraudes en medios de pago, las comisión de éstos puede entrañar como consecuencia la imposición de penas, como hemos visto en el apartado anterior. Como consecuencia, no resultan en general aplicables los procedimientos de resolución extrajudicial, que atienden más bien a cuestiones civiles (pagos excesivos, contratos incumplidos...) que a cuestiones de índole penal (represivas y ejemplarizantes). Por tanto, hay que exigir y reivindicar un procedimiento judicial adecuado a los derechos de los consumidores.

Pero no es menos cierto que en este ámbito se dan en muchas ocasiones actuaciones de las entidades en el ámbito de los medios de pago con sus clientes que “defraudan las expectativas” de éstos (prácticas abusivas, gestiones erróneas que repercuten al usuario...); por no hablar de las recurrentes imposiciones de responsabilidad al consumidor en la comisión por terceros de fraudes en medios de pagos, muchas de cuyas imposiciones vienen recogidas en los propios contratos. Pues bien, para todas estas actuaciones se deben establecer mecanismos que sean capaces de dar solución rápida, eficaz y transfronteriza a las controversias entre consumidores y entidades proveedoras de servicios de pago. En la actualidad, en el ámbito financiero existe la Red FIN-USE, una red que existe y que a veces, incluso funciona, pero que es evidente debe ser modificada.

Consumidores y resolución extrajudicial de conflictos en servicios financieros. Situación actual, perspectivas y propuestas

Debido a la continua expansión de la actividad económica en el mercado interior, cada vez son más las actividades de los consumidores que desbordan los límites de sus Estados miembros respectivos. Y esto se hace especialmente evidente en el ámbito de los medios de pago. El incremento de los desplazamientos y la utilización de nuevas tecnologías que facilitan la venta a distancia, como internet, los sistemas de comunicación móviles y la tele compra a través de la televisión digital. Estos medios aportan instrumentos prácticos para que los consumidores nacionales se conviertan en consumidores transnacionales activos. No obstante, para que los consumidores puedan aprovechar estas oportunidades debe garantizarse su participación directa y continua.

Varios instrumentos comunitarios confieren a los consumidores una serie de derechos básicos. Ahora bien, para que estos derechos tengan valor práctico, deben existir mecanismos que permitan garantizar su ejercicio efectivo. Para que los consumidores tengan la suficiente confianza para comprar en un Estado miembro distinto del suyo y puedan beneficiarse del mercado interior, deben tener la garantía de que si no están satisfechos pueden obtener indemnización. Por otra parte, la posibilidad de recurrir a mecanismos alternativos al procedimiento judicial puede evitar litigios, puesto que incita a las partes a buscar un acuerdo antes de formalizar sus problemas con un tercero. La mera existencia, pues, de estos mecanismos puede prevenir problemas.

Las nuevas tecnologías deben fomentar una red de resolución eficaz

El desarrollo de las tecnologías de la comunicación será fundamental para que los consumidores, al igual que las empresas, dispongan de los instrumentos necesarios para resolver los litigios, sobre todo si las partes se encuentran en jurisdicciones diferentes. La experiencia acumulada con los métodos tradicionales de solución de litigios será esencial para el desarrollo de procedimientos en un entorno electrónico. Entre otras cosas, ello mejora el acceso a esos mecanismos, agiliza el proceso y ofrece a las partes un mayor control del procedimiento de resolución. Las tecnologías tendrán, pues, una función cada vez más central en la resolución de litigios y podrían contribuir a ofrecer una alternativa verosímil al procedimiento judicial. Será un importante factor para consolidar la confianza de los consumidores y las empresas en el mercado interior.

Y en este sentido, la “resolución alternativa de litigios” es una cuestión fundamental que abarca una serie de órganos extrajudiciales que ofrecen una vía alternativa al procedimiento judicial, entre los que se encuentran el arbitraje, la evaluación neutra previa, el peritaje, la mediación y la conciliación.

1. Un procedimiento de resolución de conflictos, independiente, eficaz y gratuito

La Comisión Europea a través de sendas Recomendaciones (de 4 de abril de 2001 y 30 de marzo de 1998 relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de los litigios en materia de consumo, establece una serie de principios para los procedimientos de resolución extrajudiciales a nivel Europeo.

Así, todo órgano existente o que pueda crearse, que tenga como competencia la solución extrajudicial de litigios en materia de consumo, respete los principios siguientes:

Principio de independencia

Principio de independencia: La independencia del órgano responsable de la toma de la decisión estará asegurada, de forma que se garantice la imparcialidad de su acción. Cuando la decisión se adopte de forma individual, esta independencia estará garantizada, según la Comisión Europea, por las medidas siguientes:

- la persona designada tendrá la **capacidad, la experiencia y la competencia**, en particular en materia jurídica, necesarias para la función,

- la **duración del mandato de la persona designada deberá ser suficiente** para garantizar la independencia de su acción, sin que ésta pueda ser destituida sin motivo justificado,

- cuando la persona designada sea nombrada o remunerada por una asociación profesional o por una empresa, **no deberá haber trabajado para dicha asociación profesional, ni para uno de sus miembros**, ni para la empresa en cuestión, durante los tres años anteriores a su entrada en funciones.

- Cuando la decisión se adopte de forma colegial, la independencia del órgano responsable de ella puede garantizarse mediante la representación paritaria de los consumidores y de los profesionales o por el respeto de los criterios antes enunciados.

Los procedimientos deberían ser gratuitos

En segundo lugar, el Principio de transparencia, que exige que la comunicación por escrito, o en cualquier otra forma apropiada, a cualquier persona que lo solicite, de la información siguiente:

- una **descripción precisa de los tipos de litigios** que pueden someterse al órgano, así como los límites que puedan existir en relación con la cobertura territorial y el valor del objeto de los litigios,

- las **normas relativas a la consulta del órgano**, incluidas, en su caso, las gestiones previas impuestas al consumidor, así como otras normas de procedimiento, en particular las relativas al carácter escrito u oral del procedimiento, a la comparecencia personal y a las lenguas del procedimiento,

- el posible **coste del procedimiento** para las partes, incluidas las normas relativas al reparto de los costes con posterioridad al procedimiento (hay que advertir que en España, el sistema Arbitral de Consumo, salvo cuestiones probatorias, es gratuito para las partes)

- **el tipo de normas en las que se basan las decisiones del órgano (disposiciones legales, equidad, códigos de conducta, etc.)**, las modalidades de toma de decisión en el órgano, el valor jurídico de la decisión, precisando claramente si es o no de carácter obligatorio, para el profesional o para las dos partes. Si la decisión tuviera carácter obligatorio, deberán precisarse las sanciones aplicables en caso de incumplimiento de la decisión. Lo mismo se aplica a las vías de recurso que puedan existir para la parte que no obtenga satisfacción; finalmente la publicación, por el órgano competente, de un informe anual relativo a las decisiones dictadas, que permita evaluar los resultados obtenidos y determinar la naturaleza de los litigios presentados.

Hay que garantizar sistemas eficaces para resolver problemas de índole financiera

En tercer lugar, el **Principio de contradicción**, según el cual la Comisión entiende que el procedimiento que habrá de seguirse implicará la posibilidad de que todas las partes interesadas den a conocer su punto de vista a la institución competente y que tengan conocimiento de todas las posturas y de todos los hechos expuestos por la otra parte, así como, en su caso, de las declaraciones de los expertos.

El objetivo: procedimientos eficaces que se cumplan

Otro principio esgrimido por la Comisión en estas Recomendaciones para la resolución extrajudicial de con-

flictos con consumidores es el **Principio de eficacia** que estará asegurada por medidas que garanticen el acceso del consumidor al procedimiento, sin estar obligado a utilizar un representante legal; la gratuidad del procedimiento o la fijación de costes moderados; la fijación de plazos cortos entre la consulta presentada ante el órgano y la toma de la decisión; y- la atribución de un papel activo al órgano competente, que le permita tener en cuenta todo elemento útil para la solución del litigio.

Buenos criterios pero sin aplicación efectiva

El Principio de legalidad, según el cual, en caso de litigios transfronterizos, la decisión del órgano no podrá tener como resultado privar al consumidor de la protección que le garantizan las disposiciones imperativas de la ley del Estado miembro en el cual el consumidor tenga su residencia habitual, en los asuntos previstos en el artículo 5 del Convenio de Roma de 19 de junio de 1980 sobre la ley aplicable a las obligaciones contractuales. Toda decisión se justificará y comunicará por escrito, o de cualquier otra forma apropiada, a las partes interesadas, en el menor plazo posible. El Principio de libertad: La decisión del órgano sólo podrá ser obligatoria para las partes cuando éstas hayan sido previamente informadas y la hayan aceptado expresamente. La adhesión del consumidor al procedimiento extrajudicial no podrá ser resultado de un compromiso anterior al surgimiento de un desacuerdo, cuando dicho compromiso tenga por efecto privar al consumidor de su derecho a recurrir a los órganos jurisdiccionales competentes para la solución judicial del litigio.

Y por último, el Principio de representación: El procedimiento no podrá privar a las partes del derecho a hacerse representar o acompañar por un tercero en toda las etapas del procedimiento.

2. Los países europeos disponen de heterogéneos e insuficientes sistemas para resolver la mayoría de los conflictos de consumo

Pese a estos principios, en la mayor parte de los Estados miembros del Espacio Económico Europeo (EEE) existen procedimientos de resolución extrajudicial de denuncias sobre servicios financieros muy dispares. Su objetivo es resolver los litigios entre usuarios y su proveedor de servicios financieros, es decir, banco, compañía de seguros, organismo de inversión u otra entidad financiera. Estos procedimientos pretenden constituir una manera rápida, económica y sencilla de resolver los conflictos, pero los procedimientos de denuncia extrajudicial son procedimientos alternativos y voluntarios, cuyos resultados no tienen por qué ser totalmente comparables a los fallos de los tribunales y, por lo tanto, no sustituyen a los procedimientos judiciales.

El recurso a los tribunales no adecuado para los consumidores

Los procedimientos judiciales normales son a menudo incómodos y pueden tardar mucho tiempo. Los procedimientos extrajudiciales pretenden ofrecer una manera alternativa de solucionar sus conflictos rápida, económica y fácilmente, lo cual sólo en ocasiones puede evitar la necesidad de acudir a los tribunales. Los órganos que tramitan las denuncias suelen ser órganos propios de las entidades financieras y, sus decisiones, por extraño que pueda parecer, no son en todos los sistemas vinculantes para las empresas, la mayoría tiende a atenerse a ellas. Se podría decir que la Red funciona, pero sólo en ocasiones resuelve los problemas de los consumidores.

Los nuevos instrumentos de actuación de la Comunidad, entre ellos el Tercer Plan de Acción (1996-1998) en materia de política de consumo, intensificaron una visión más certera en la consideración del consumidor no únicamente como una circunstancia necesaria del mercado, sino, sobre todo, como un ciudadano con necesidad de ver protegidos sus derechos en todo el marco político, económico y social del sistema de la construcción europea, a través de medidas de corrección en los ámbitos de los servicios públicos, los servicios financieros, la seguridad alimentaria y el pujante nacimiento de la sociedad de la información en el marco de un consumo sostenible.

Las reformas operadas en Amsterdam entre el 17 y el 18 de junio de 1997, suponen un posicionamiento más firme de la Comunidad en la promoción de la política de consumo, incluyendo la posibilidad de supervisar las políticas internas de los Estados, integrando, en una posición de horizontalidad, al consumo en el resto de políticas comunitarias, aunque, en el conocido paso adelante y paso atrás que ha caracterizado la construcción europea, se echó en falta un expreso reconocimiento en el nuevo articulado (art. 153 TCE) una mención explícita al derecho de defensa de los intereses de los consumidores para la reparación de los daños y el acceso a la justicia.

En todo caso, es pertinente señalar que a partir de Amsterdam surge con fuerza la contemplación del acceso de los consumidores a sistemas eficaces de recurso y solución de litigios, y, en este contexto, en materia de acciones de cesación y órganos responsables de la resolución extrajudicial de litigios, se comienza un trabajo que contempla los principios de independencia, transparencia, contradicción, eficacia, legalidad, libertad y representación, como esenciales para el afianzamiento de las garantías de los consumidores.

La solución extrajudicial de conflictos y el especial tratamiento de los servicios financieros

La preocupación por la necesidad de establecer un marco concreto de resolución judicial de conflictos no ha cesado en estos años. A partir de 2000, y como continuación al trabajo efectuado a finales de la anterior década, se ha promovido un desarrollo de diversos instrumentos de resolución extrajudicial de conflictos que viene funcionando desde entonces con relativa normalidad.

Con apoyo en la triple fórmula de la conciliación, la mediación y el arbitraje, la Comisión Europea, a partir de su Comunicación sobre la solución extrajudicial de los conflictos en materia de consumo, promovió un modelo avanzado que permitiera caminar hacia un sistema consensuado de mediación, y, también, hacia una coordinación eficaz entre tal mediación y el ámbito jurisdiccional.

En esta época se han ensayado también soluciones que, actualmente, forman parte del paisaje de la solución extrajudicial de conflictos, tal es el caso de la Red EJE, que tenía por objetivo básico permitir una solución rápida y eficaz de los tan citados litigios de consumo, que, una vez fusionada con la Red Euroventanillas, dio lugar a los actuales Centros Europeos de Consumidores “Red CEC”.

Estos CEC, entre otras cuestiones, tienen como misión ayudar y apoyar a los consumidores en sus contactos con el comerciante reclamado y ayudar al consumidor, si fuera necesario, con motivo de una denuncia, queja o reclamación. Y, asimismo, en idéntico orden de cosas, tales centros mantienen una directa relación con FIN – NET, el sistema extrajudicial de resolución de litigios financieros transfronterizos.

Situación actual y perspectivas del sistema FIN – NET

Este sistema fue creado a partir de febrero de 2001 por la Comisión Europea con la misión de proporcionar un acceso sencillo y documentado a la resolución extrajudicial de conflictos transfronterizos, garantizando el intercambio de informaciones entre los Estados miembros, y tratando de armonizar los principios sobre los que debían bascular los sistemas extrajudiciales de resolución de conflictos en los ordenamientos nacionales.

Actualmente el sistema cuenta con participación de 46 entidades de 21 Estados miembros, según informa su propia página web, y se dedica esencialmente a la resolución de cuestiones transfronterizas en materia de servicios financieros, entendiendo como tales los que afectan a servicios bancarios, seguros y mercado de valores, priorizando el denominado sistema más cercano, que redunda en que el consumidor acuda al sistema extrajudicial de su Estado miembro de residencia, aun cuando su reclamación se dirija a una sociedad financiera extranjera.

En este caso, una vez disponga el consumidor de toda

la información sobre el trámite a desarrollar en cada caso, podrá presentar una reclamación en su sistema extrajudicial, el cual la derivará al que tenga competencia según la normativa vigente.

En España la responsabilidad del mantenimiento de la Red Fin – Net recae sobre el Servicio de Reclamaciones del Banco de España. Según informa éste en su última Memoria de Actividades, los grandes bancos concentran el mayor número de reclamaciones, constriñéndose al ámbito mediterráneo las que afectan a las cajas de ahorro, situación igualmente comprensible en función de las determinaciones de residencia de los ciudadanos europeos.

3. **Ante el “frenazo de Europa”, un sistema efectivo generaría la necesaria confianza entre los usuarios europeos**

Extraer conclusiones en estos momentos de la construcción europea sobre algunos de los aspectos que más directamente afectan al ciudadano – consumidor europeo, es, sin lugar a dudas, entrar en un panorama sombrío, como es el propio momento por el que atraviesa tal construcción.

En los últimos años hemos asistido a lo que aparenta ser un constante retraimiento de la construcción europea a favor de un mayor protagonismo de los Estados.

Un verdadero papel protagónico de las instituciones comunitarias sería deseable en un marco general de libre circulación de mercancías, capitales, servicios y personas. Una presencia más activa de los órganos político – administrativos de la Unión permitiría a los ciudadanos visualizar con mayor potencia la presencia de ésta en nuestras vidas.

Frente a ello, el panorama observado se presenta como una incipiente voluntad, no materializada, de seguir avanzando, si bien con las ideas poco claras de cómo superar el estigma de las reticencias internas a perder soberanía a favor del proyecto común.

La integración de la Unión Europea avanza tan lenta como la protección de los usuarios

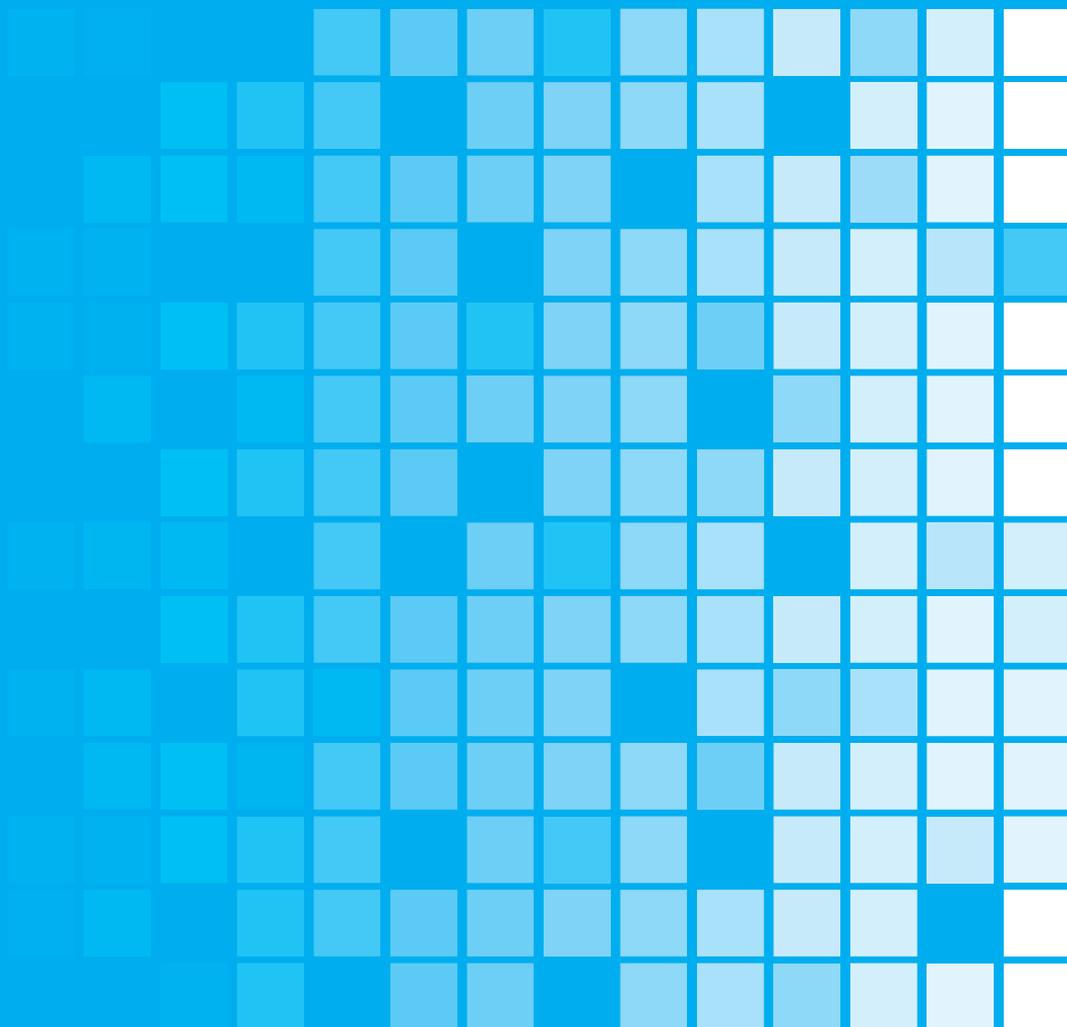
En el caso de la solución extrajudicial de conflictos, y en el concreto ámbito de los servicios financieros, las noticias tampoco son espectaculares. Pues si reticentes son los Estados a dotar a la Unión de verdaderos poderes en la organización, control y supervisión de los mercados, más los son los grandes capitales y las gigantes empresas inmersas en el marco financiero de aquellos, a someterse a los sistemas de solución extrajudicial de conflictos.

Los defectos están a la vista. La nula voluntad de los Estados por compeler a bancos, aseguradoras y demás entidades financieras y de crédito a someterse a estos sistemas, desde luego no contribuye a que las cosas mejoren. El papel normativo de la Unión, como decimos, está reducido a un cúmulo de buenas intenciones, con el que chocan, a menudo, los intereses internos de los Estados y los económicos de las multinacionales que operan en este mercado. Parece por tanto, el actual sistema aquí descrito, muy insuficiente para las verdaderas y justas demandas de los consumidores de los Estados miembros.

Las perspectivas, por otro lado, tampoco parecen ser muy halagüeñas. En la proverbial manera de construir Europa con un paso para adelante y dos para atrás, no parece muy cercana una verdadera modificación en los centros normativos para dotar a la solución de conflictos en el ámbito de los servicios financieros de una cierta potencia ejecutiva. Los tímidos avances en la regulación comunitaria en los últimos años, unidos a la palmaria falta de interés de los Estados en trasponer estas Directivas, no permite aventurar grandes éxitos en los próximos años. De ahí la necesidad de contar con las organizaciones de la sociedad civil, portadoras de las verdaderas inquietudes de los ciudadanos y sus problemas, y en el ámbito que tratamos, con las asociaciones de consumidores

Ver fichas comparativas con la situación de los sistemas extrajudiciales de resolución de conflictos en los distintos países partners en el anexo III.

Conclusiones y propuestas



Conclusiones: el mercado único de los medios de pago necesita de la seguridad y confianza de los consumidores y la participación en su diseño de sus asociaciones

De todo lo planteado hasta ahora no cabe duda de que el ámbito de los medios pagos se encuentra en una fase de renovación radical debido a los progresos generales tecnológicos y de mercado. Unos progresos que también producen riesgos. Por ello, la primera conclusión que debe extraerse es que la legislación actual sobre pagos y protección al usuario de los mismos, no es aún suficiente y apropiada para establecer el marco adecuado de garantía para el consumidor. La evolución tecnológica debe venir acompañada de una evolución jurídica en el mismo sentido e intensidad, con nuevos mecanismos de supervisión, nuevas figuras normativas y sobre todo, mayor participación de los consumidores a través de sus Asociaciones a la hora de definir y establecer estas nuevas pautas legales.

Hay que advertir igualmente que la desconfianza de los consumidores hacia los medios de pago no proviene únicamente de la comisión de fraudes delictivos por parte de terceros. Los costes razonables en su uso, un equilibrio justo en las contraprestaciones recogidas en contratos (en los casos de fraude se hace recaer toda la responsabilidad y consecuencias en el usuario, eximiéndose totalmente la entidad) y un sistema de solución de conflictos rápido y eficaz en su resoluciones, son algunas de las medidas que deben completar una reordenación normativa nueva de los medios de pago.

De poco serviría establecer unos mecanismos jurídicos adecuados para combatir las estafas en los medios de pago si las actuaciones de las entidades financieras emisoras de medios de pago siguen generando desconfianza en los usuarios por costes, interpretaciones interesadas de los contratos, etc.

Por eso, como conclusiones, las actuaciones futuras para mejorar la protección de los intereses de los consumidores y usuarios en el ámbito de los fraudes en medios de pago, debería establecerse conforme a tres principios: principio de seguridad técnica, principio de seguridad jurídica para el consumidor, y principio de cooperación efectiva entre sector público, empresas y Asociaciones de Consumidores.

1. Principio de Seguridad Técnica

- Establecimiento a nivel Europeo y Estatal, de unos principios mínimos que permitan establecer en el sector privado un **Plan de Inversiones Financieras para garantizar unos mínimos anual de dotaciones para prevenir y combatir los fraudes en me-**

dios de pago. Dada su repercusión e importancia social y económica, no puede quedar en manos de las propias empresas exclusivamente.

- Creación de un **Plan uniforme para la evaluación y control de los sistemas y medios de pago que las entidades ponen en el mercado**, así como de los medios a través de los cuáles éstos son utilizados (cajeros, terminales de punto de venta, páginas web de las entidades...). Deben cumplirse unos mínimos estándares de seguridad, siempre sometidos a revisión y control, que permita su mejora, así como la puesta en común de los defectos y potenciales errores detectados.

- Creación de una **Autoridad en la materia a nivel europeo, una organismo de supervisión con Unidades especiales para la Inspección de estos sistemas operativos de pago**, a través de órganos técnicos adecuados en los organismos financieros supervisores. Su función, que debería establecerse por la Unión Europea, permitiría evaluar y comprobar las garantías que ofrecen los medios de pago puestos a disposición de los consumidores por las entidades.

- **Nuevas modalidades rápidas y efectivas de comunicación y notificación de pérdidas y robos de tarjetas**, que aseguren que operaciones fraudulentas hechas con posterioridad a dicha comunicación dejen de tener validez. Este sistema debería ser operativo los 365 días del año, teniendo en cuenta que un gran porcentaje de fraudes se comenten los fines de semana.

- **Nuevas herramientas y sistemas que hagan mucho más difícil el fraude. La utilización de memorias externas suministradas por las propias entidades a sus clientes usuarios de banca electrónica con el software necesario** para la utilización de este servicio con la total seguridad y certeza de que sus datos y operaciones no pueden ser interceptadas por malware, troyanos, virus, etc. También sería necesario la obligatoriedad de una doble aceptación de la operación por dos sistemas diferentes, por ejemplo, en el caso de comercio electrónico aceptar el pago a través de la red y confirmarlo con un mensaje de teléfono móvil.

2. Principio de Seguridad Jurídica para los consumidores

- Dado que se trata de ilícitos transnacionales, hay que superar la falta de homogeneidad en la actual legislación. La unificación de las medidas legales (preventivas, represivas y resarcidoras) exige una **aproximación de las normativas estatales bajo el principio de máxima protección al consumidor como criterio**. En algunos países el mero hecho de poseer aparatos copiadore de medios de pago, por ejemplo las tarjetas, ya es constitutivo de delito, mientras que en otros no.

- Por ello, debería ser necesario **un control previo en toda la Unión de la venta de estos aparatos**, otorgando una licencia que autorice a la empresa o persona que posea estos aparatos a poder producir lícitamente medios de pago, por lo que la mera posesión sin licencia sea constitutiva de sanción al menos administrativa. **Porque a los consumidores lo que les interesa no son tanto las medidas represivas contra el autor/es, sino el resarcimiento de su perjuicio económico; si bien es cierto que el aspecto penal debería incidir como medida disuasoria y, por consiguiente preventiva.**

- Establecimiento de **medidas penales uniformes a nivel europeo para estos delitos, conforme a penas efectivas, justas y disuasorias.**

- A ello debe añadirse un **mejora en la cooperación judicial y procesal entre países**. Los delincuentes conocedores de la normativa cometen el fraude teniendo en cuenta las consecuencias que puede tener esto, cometiendo fraudes de una determinada cantidad que no sean constitutivos de delito sino de falta, con lo que sus sanciones son diferentes. Por ello, y debido a este comportamiento el legislador europeo debería actuar en consecuencia para evitar estas triquiñuelas legales.

- Dado que se trata de un ámbito con **escasa regulación hasta el momento, y que la existente ha sido de cumplimiento “voluntario” por las entidades** (con las consecuencias de inseguridad para los consumidores) es necesario dotar de un cuerpo normativo obligatorio a nivel Europeo específico y concreto para las operaciones en medios de pago. **Una futura Directiva, al igual que la existente en el ámbito del Crédito al Consumo, donde se recojan y regulen adecuadamente todas las prácticas abusivas llevadas a cabo por las entidades financieras en el sector de medios de pago.** En este sentido, el presente estudio puede convertirse en una herramienta eficaz.

- Consecuencia de estas “normas blandas”, la cláusulas abusivas y desproporcionadas para los derechos del consumidor han sido habituales en los contratos en medios de pago. **Una futura Directiva de derechos del consumidor en los medios de pago debe establecer una regulación detallada de estas cláusulas, así como el establecimiento de control previo de los contratos** para filtrarlas e imponer su no inclusión, tasando y regulando concretamente la responsabilidad de las partes ante un posible fraude, y no dejándolo, como sucede en la actualidad, a la “voluntad de las partes” que, como ya hemos tenido ocasión de comprobar en este Estudio, sólo es la voluntad de el preponente del contrato, es decir, la entidad emisora del medio de pago o proveedora del mismo.

- Los usuarios de los servicios de pago consideran que algunas operaciones de pago -especialmente en el actual entorno tecnológico- deberían ofrecerse a un **precio marginalmente bajo y casi en tiempo real**. Es fundamental que se establezcan a nivel europeo criterios básicos para el cobro de comisiones por estos servicios, aplicando criterios de transparencia y justicia que no supongan para el consumidor una desproporción o abusos en el cobro por su uso.

3. Principio de Cooperación efectiva entre el sector privado, las autoridades públicas y las organizaciones de consumidores

- La Comisión Europea debe **impulsar la creación de un órgano de cooperación y supervisión que sirva como canal de diálogo entre estos sectores, pero reforzando la posición de los consumidores y sus organizaciones**. A través de este Foro de los Medios de pago se deben debatir propuestas de mejora, analizar la normativa, asesorar a los órganos de la Unión Europea con competencia en este ámbito, etc.

- Creación de un sistema de **Red de Alerta de fraudes en medios de pago**, que cuando suceda un caso de fraude permita comunicarlo a los organismos públicos, privados y asociaciones de consumidores de los distintos Estados miembros, informando rápidamente a los consumidores del ataque, sus características y riesgos.

- La Comisión Europea debería impulsar **una gran campaña informativa, de gran difusión, a través de las Asociaciones de Consumidores Europeas**, que llegue a todos los consumidores y usuarios de medios de pago, y donde se les prevenga de los riesgos y consecuencias de los fraudes, cómo prevenirlos y evitarlos.

Resumen de conclusiones

■ **Establecer una normativa y una regulación acorde a las necesidades del usuario de medios de pago**

- *Dotar de un cuerpo normativo obligatorio a nivel europeo donde se recojan y regulen adecuadamente todas las prácticas abusivas llevadas a cabo por las entidades bancarias.*
- *Establecer un equilibrio justo en las contraprestaciones recogidas en los contratos de las tarjetas, ya que en los casos de fraude se hace recaer toda la responsabilidad al usuario.*
- *Homogeneizar unos criterios básicos para el cobro de comisiones en todos los países de la Unión Europea, a un precio marginalmente bajo y casi en tiempo real.*

■ **Cooperación del sector privado, las autoridades públicas y las organizaciones de consumidores**

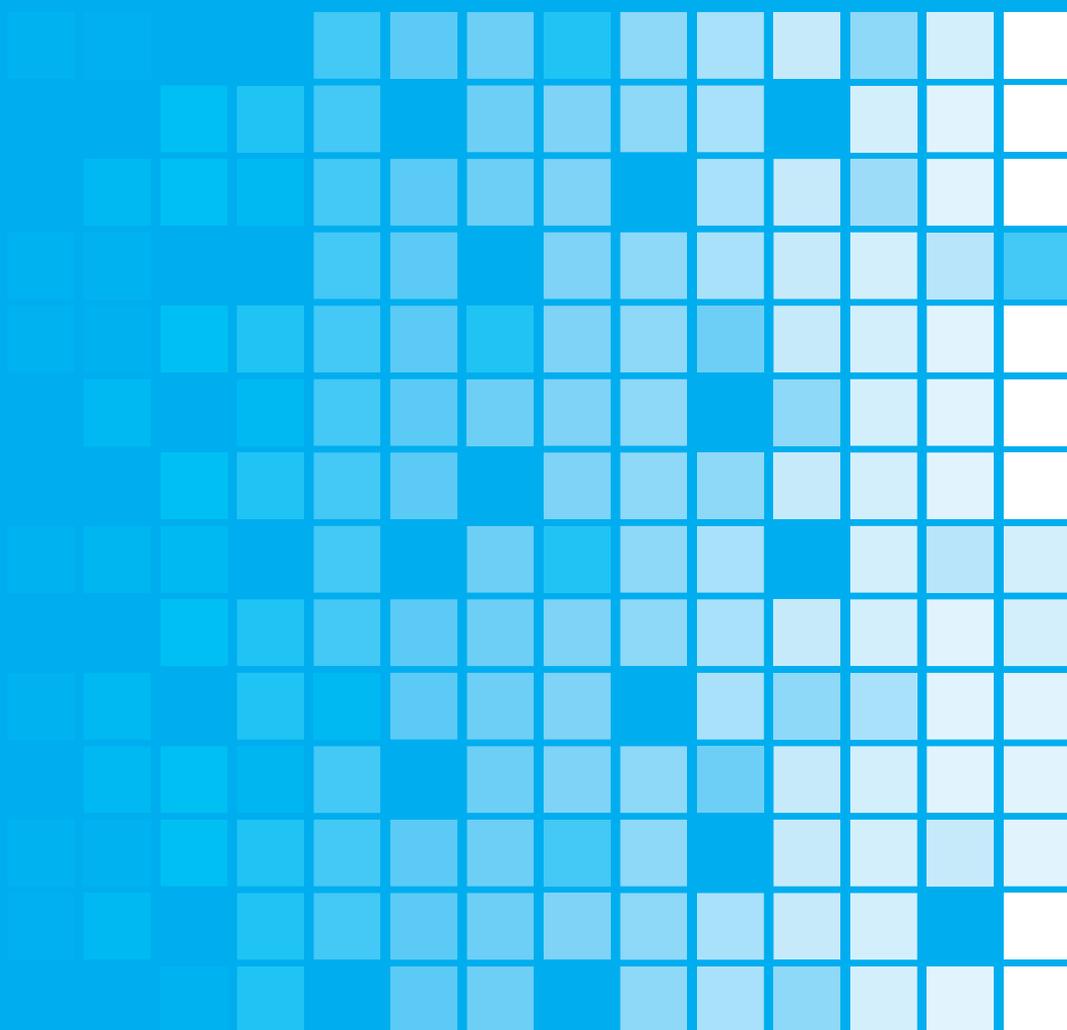
- *Creación de un sistema de alerta que permita informar rápidamente a los consumidores de los fraudes cometidos.*
- *Impulsar una gran campaña informativa por parte de la Comisión Europea a través de las Asociaciones de Consumidores Europeas.*

■ **Establecer una serie de iniciativas de índole técnico u administrativo que garanticen unas transacciones seguras**

- *Organismo de supervisión que permita evaluar y comprobar las garantías de seguridad que ofrecen los medios de pago.*
- *Nuevas modalidades rápidas y efectivas de notificación de pérdidas y robos de tarjeta.*
- *Herramientas y sistemas que dificulten el fraude y que sean suministradas por las entidades bancarias a sus clientes.*

Anexo I

Sentencias judiciales sobre fraudes en medios de pago



Tarjetas bancarias: los tribunales exigen mayor diligencia a bancos y cajas de ahorros

De los distintos países participantes en el proyecto sobre fraudes encabezado por ADICAE, presentamos a continuación un anexo con los aspectos fundamentales de su normativa para hacer frente a los problemas a que se enfrentan los consumidores en tales países. La conclusión es clara, hace falta una normativa común y lo más cohesionada posible.

RESPONSABILIDAD Y CARGA DE LA PRUEBA POR EXTRAVÍO Y/O USO FRAUDULENTO DE LA TARJETA BANCARIA

Como se ha puesto de manifiesto en el epígrafe referente a las cláusulas abusivas, el usuario tal y como se prevé en la Recomendación y en la Directiva europea sobre medios de pago soportará las pérdidas derivadas de las operaciones de pago no autorizadas resultantes de la utilización de su tarjeta extraviada o sustraída, hasta un máximo de 150 €. Una vez comunicada la incidencia. Salvo en los supuestos de uso fraudulento por su titular, éste, una vez comunicada la incidencia, no soportará consecuencia económica alguna.

No obstante, lo expuesto con anterioridad, el emisor de la tarjeta será responsable, incluso con anterioridad a la notificación, cuando no hubiese puesto en todo momento a disposición de su cliente todos los medios adecuados para que este hubiese podido notificarle a la mayor brevedad posible el extravío o sustracción de la misma.

SAP de Alicante, Sección 9ª, de 30 de marzo de 2007: las tarjetas no tienen regulación específica

“Los contratos de Tarjetas de crédito son considerados por la doctrina, contratos atípicos por cuanto no tienen una regulación legal específica, de ahí la importancia que para su regulación tiene la voluntad de las partes (art. 1255 del CC), pero tampoco podemos olvidar que como contratos bancarios que son, tienen la condición de contratos de adhesión cuyas cláusulas son impuestas por una entidad bancaria, que las remite al cliente quien las suscribe de forma global, sin negociación ninguna, por lo que en cualquier caso la interpretación de su contenido deberá en cualquier caso, acogerse a la Ley 26/1984, General para la Defensa de los Consumidores y Usuarios. Por otra parte la doctrina ha venido recogiendo con carácter general, el criterio de establecer como de cargo de la Entidad emisora de la tarjeta, la prueba de la culpa grave del usuario o titular; así se recoge por la SAP de Asturias de 15 de febrero de 2005, a la que expresamente se refiere la SAP de Madrid de 25 de abril de 2006: La Recomendación 87/598 de 8 de diciembre de 1987 de la Unión Europea sobre el Código de buena conducta en materia de pago electrónico y la 97/489 de 30 de julio de 1997 que la revisa y actualiza, contemplan la responsabilidad del titular de la tarjeta durante el tiempo que media entre su pérdida o sustracción ilegítima hasta la notificación de este hecho al emisor en solo 150 euros, excepto cuando haya actuado de forma fraudulenta o negligentemente grave, (en cuyo caso no se aplicará dicho límite), en el cumplimiento de sus obligaciones de uso y cuidado adecuados del instrumento electrónico, mantenimiento del secreto sobre su PIN o demora en la notificación al emisor de la pérdida, sustracción o falsificación del instrumento electrónico (artículo 8.3 de la primera y 6 de la segunda). El Servicio de Reclamaciones del Banco de España, a partir de 1991, comienza a informar como no ajustado a las buenas prácticas bancarias no aplicar al titular de la tarjeta el límite de responsabilidad referido (informes relativos a las reclamaciones 1334/91, 1514/91 y 25/92) y así es que, desde entonces, ha venido incorporándose a los contratos bancarios de tarjeta”.

La carga de la prueba se desplaza a la entidad emisora de las tarjetas, por ser ésta la que mayor facilidad probatoria tiene al disponer de los medios a su alcance para rastrear los movimientos realizados con las tarjetas, también los Tribunales cargan a las Entidades Financieras con la responsabilidad de resarcir al usuario, con las salvedades debidas.

SAP de Valencia, núm. 200/2006, de 17 de mayo de 2006: el riesgo lo deben asumir las entidades

“(…) las consecuencias perjudiciales que pueden derivar de tal riesgo en principio han de ser asumidas por las entidades bancarias pues son ellas la parte fuerte o dominante del contrato, las generadoras de la fuente del riesgo dado que son las que emiten las tarjetas e impulsan su uso en masa; las que marcan las reglas de funcionamiento y seguridad de la propia tarjeta fijadas en el propio contrato de adhesión y por último porque controlan y confeccionan

los medios tecnológicos desplegados para su efectividad y su seguridad, pues son las que han configurado en el punto ahora que interesa, los cajeros automáticos, su ubicación y sus medidas de seguridad. Tal asunción de ese riesgo técnico determina la responsabilidad de las entidades bancarias tal como se reconoce por la mayoría de la Jurisprudencia (Sentencia Audiencia Provincial Madrid, sección undécima 7-12-2002; Asturias 18-3-2002, y Tarragona, sección tercera, 27-12-2004, ésta última en un supuesto fáctico semejante al ahora enjuiciado) a no ser que el perjuicio causado sea imputable al titular de la tarjeta (...)

En el párrafo siguiente la misma Sentencia hace un reparto de los derechos y obligaciones de ambas partes -cliente y entidad- que nos parece muy explicativo: “El titular de la tarjeta como se establece en las condiciones del contrato ostenta como obligaciones la conservación correcta y con precaución de la tarjeta y mantener en secreto el PIN; no anotar el PIN en la tarjeta ni en documento que se lleve o transporte junto dicha tarjeta y notificar de forma inmediata la pérdida, robo o falsificación de la tarjeta y el conocimiento por otras personas contra su voluntad del número de Identificación personal. Por su parte la entidad Bancaria se obliga a mantener secreto el PIN y anular las tarjetas Caducadas y denunciadas, entre otros extremos porque el PIN sea conocido por persona distinta a su titular. La diligencia en el cumplimiento de esas obligaciones no puede tener el mismo rasero, pues la del cliente - consumidor conforme al artículo 1104 del Código Civil ha de ser la genérica de un padre de familia, atemperada siempre a las obligaciones impuestas y explicitadas en el contrato suscrito, mientras que la diligencia de la entidad bancaria es la exigible a un profesional, dado que es la entidad bancaria la que confecciona el sistema y dispone al caso de los cajeros, su diseño y medidas de seguridad, por ende en mayor disposición para corregir los fallos que se producen en dicha seguridad Sentado ello corresponde conforme las reglas de la carga probatoria fijadas en el artículo 217 de la Ley Enjuiciamiento Civil, a la entidades bancaria acreditar que el cliente ha sido negligente o no ha tenido la diligencia exigible en la conservación de la tarjeta o en guardar secreto del PIN (asi sentado en sentencias Audiencia Provincial Toledo 1/7/1999, Málaga (sección sexta)23/7/2002 y Madrid (sección 12ª) 6/10/2004, mientras que corresponde al usuario de la tarjeta acreditar que las disposiciones efectuadas con su tarjeta son fraudulentas, es decir no realizadas por él ni tampoco con su autorización, distribución de la carga probatoria respetada por la Juez de Instancia. En consecuencia, caso de constatar esas disposiciones no autorizadas por tercero y obtenidas de forma ilícita, sólo el titular de la tarjeta será responsable en caso de un uso negligente o falta del deber de diligencia en las obligaciones de custodia y secreto, pues fuera de tales casos el riesgo técnico tendrá que ser asumido por la parte fuerte contratante y que impulsa el sistema (criterio igualmente fijado en la sentencia de Audiencia Provincial Murcia -sección primera-29/9/2004).

SAP de Zaragoza, de 28 de marzo de 2006: problemas y responsabilidades tras el robo de tarjeta

“La cuestión (...) radica en determinar quién debe asumir los riesgos derivados del uso fraudulento de la tarjeta de crédito sustraída a la consumidora actora Todo ello a partir de la sucesión de disposiciones -un reintegro de 300 euros a las 18,58 horas del día 1-11-03, otro igual de 300 euros 1 minuto mas tarde y 3 minutos mas tarde una recarga telefónica de 100 euros- encadenadas tras un único intento fallido a las 18,44 horas, por marcaje erróneo del número secreto(...)

El Juez de Primera instancia concluyó que si el delincuente accedió con tanta facilidad a ese número, a tiempo tan escaso de la sustracción del billeteo, fue por obrar el mismo en éste, lo que supuso una infracción de la obligación de reserva de la clave secreta o número de identificación personal, hecho que, por la grave negligencia que representa, activa la obligación de la titular de la tarjeta de asumir íntegramente la pérdida de tales operaciones.

No obstante, inferir en esa vía presuntiva que la actora tenía anotado el número secreto en alguno de los documentos obrantes en el billeteo, ello con la única base proporcionada por la rapidez y precisión con que las operaciones se ejecutaron hay que concluir que resulta aventurado, pues no es solo que lo que hoy en día cabe presumir es que nadie lleva el número secreto así apuntado.

La imposible averiguación del número PIN en ese tiempo es solamente una alegación interesada, solo sustentada en afirmaciones realizadas en documentación bancaria, que en principio parece desmentida por la experiencia diaria.

En definitiva, no pudiendo estimarse probada la negligencia de la titular de la tarjeta ni la infalibilidad del sistema respecto a la imposible obtención del PIN, debe rechazarse que el importe de los daños causados por el uso fraudulento de la tarjeta de crédito sea imputable a la consumidora.”

SENTENCIA DE LA SALA II DEL TRIBUNAL SUPREMO DE 8 DE JULIO DE 2002:

FALSIFICACIÓN DE TARJETAS Y EL FRAUDE**Resumen de los hechos acaecidos**

Los hechos declarados probados en la sentencia de la Sala de lo Penal de la Audiencia Nacional, que la Sala II del Tribunal Supremo acepta, son los siguientes:

Varios sujetos, de las cuales sólo se juzga a Óscar E.B., copian el contenido de las bandas magnéticas originales de varias tarjetas de crédito, para ser utilizadas por sus legítimos titulares en establecimientos comerciales, mediante un aparato grabador fabricado al efecto por persona desconocida y, con el mismo instrumento, copian la información en la banda magnética en blanco de otras tarjetas de crédito: unas expedidas a favor de Óscar E.B.; otras a facilitadas por terceras personas, entre ellas María del Carmen B.C.

Con las tarjetas alteradas realizaron numerosas compras. Tales hechos fueron calificados en la sentencia de la Audiencia Nacional como constitutivos de un delito continuado de falsificación de moneda de los artículos 386.1.º, 387 y 74 en concurso medial del artículo 77.1 con un delito continuado de estafa de los artículos 248.1, 250 6.º y 74, todos ellos del vigente CP, imponiendo a Óscar E.B. las penas de diez años de prisión y multa de 15.000.000 de pesetas, y a María del Carmen B.C. las penas de dos años de prisión y multa de 500.000 pesetas. Interpuesto recurso de casación por diferentes motivos, la sentencia de la Sala II del Tribunal Supremo mantuvo la misma postura dejando, sin embargo, sin efecto las penas de multa que venían impuestas conjuntamente con las de prisión.

La sustitución de los datos de las bandas magnéticas de las tarjetas

La sustitución de los datos de las bandas magnéticas de las tarjetas de crédito había sido calificada en la sentencia de la Audiencia Nacional como constitutiva de un delito de falsificación de moneda de los artículos 386.1.º y 387 del CP. A tenor del párrafo primero del artículo 386, “será castigado con las penas de prisión de ocho a doce años y multa del tanto al décuplo del valor aparente de la moneda”:

- 1.º El que fabrique moneda falsa;
- 2.º El que la introduzca en el país; y
- 3.º El que la expendia o distribuya en connivencia con los falsificadores o introductores”.

La consideración como moneda a efectos punitivos de las tarjetas de crédito, las de débito y los cheques de viaje que hace el artículo 387 es una novedad del vigente Código Penal.

Argumentos utilizados

La incorporación a la banda magnética de una tarjeta de unos datos obtenidos fraudulentamente constituye un proceso de fabricación o elaboración. La generación de un documento nuevo, sin existencia previa, como es el caso, ha de considerarse “fabricación” y no simple “alteración”, pues precisamente el elemento esencial en la tarjeta es la banda magnética.

Sin entrar a discutir si la banda magnética es el elemento esencial o lo son también otros, parece que más que generar un documento nuevo se da lugar a un documento distinto.

La voluntad del legislador no parece otra que la de la severa represión de estas acciones, atendiendo a la importancia económica actual de las tarjetas como instrumentos de pago.

Este argumento es confuso, puesto que lo que en última instancia se viene a decir es que el legislador, considerando que la gravedad de la fabricación o creación ex novo (el daño generado por la misma) y la de la mera alteración de una tarjeta de crédito son coincidentes, ha querido equiparar tales comportamientos a efectos punitivos (como ocurre en el caso de la falsedad documental).

Calificación jurídica del uso de tarjetas de crédito o de débito con la finalidad de obtener un beneficio económico ilícito

La sentencia de la Audiencia Nacional había calificado ese comportamiento como constitutivo de un delito continuado de estafa que reviste especial gravedad, tipificado en los artículos 248.1, 250 6.º y 74, todos del CP. En los recursos de casación se defienden dos alternativas: la calificación de aquel uso como delito de robo con fuerza en las cosas de los artículos 237, 238.4.º y 239, todos del CP; o la calificación de todo el comportamiento enjuiciado —falsificación de la tarjeta y posterior uso de la misma con finalidad defraudatoria— como una estafa del artículo 248.2 del CP.

La sentencia de casación, confirmando en este extremo la sentencia recurrida, descarta la primera de aquellas alternativas —robo con fuerza en las cosas— poniendo de manifiesto que en el delito de robo la fuerza en las cosas se emplea para acceder al lugar en que se encuentran los bienes que van a ser objeto de apoderamiento, todo ello sin necesidad del concurso de otra persona, lo que no ocurre en el presente caso en el que la tarjeta se utiliza para que otra persona (engañada, y por tanto equivocada) ponga a disposición del que la utiliza determinados bienes, con el consiguiente perjuicio, sea este suyo (si finalmente se ve obligado a reintegrar el precio cobrado) o de otro —empresa que comercializa el instrumento de pago (que no percibe el dinero abonado al comerciante a través de la tarjeta) o titular de la tarjeta alterada (en cuya cuenta se carga la compra).

La disquisición de la sentencia de casación está en consonancia con la jurisprudencia del Tribunal Supremo, que:

1.º Considera que la fuerza en las cosas se utiliza para acceder al lugar en el que se encuentran los bienes objeto del apoderamiento y estima como robo con fuerza en las cosas —artículos 237, 238.4.º y 239 del CP— la utilización por los no titulares de tarjetas en los cajeros automáticos .

2.º Por otro lado, cuando la tarjeta de crédito es utilizada por los no titulares en comercios, ignorando el comerciante esa circunstancia, el hecho se califica como constitutivo de un delito de estafa genérica —artículo 248.1 del CP en concurso ideal, artículo 77 del CP— con un delito de falsedad en documento mercantil —artículos 392 y 390.1 del CP—, este último derivado de la firma del talón de compra imitando la del titular legítimo o de otra alteración típica de la verdad.

Asimismo, también confirmando el criterio de la sentencia de instancia, descarta la sentencia de casación la existencia del delito de estafa del 248.2 CP —estafa informática— y que esta infracción absorba tanto la alteración de la tarjeta como el posterior uso de la misma.

La conducta tipificada en el artículo 248.2 del CP, aún incardinado este en la sección de las estafas, contempla supuestos en los que no se engaña directamente a una persona, sino que la disposición patrimonial tiene lugar llevando a cabo manipulaciones o artificios semejantes en el manejo de una máquina, lo cual, en definitiva, supone una ruptura con el concepto clásico o tradicional de la estafa.

Sin embargo, discrepamos de dicha sentencia en cuanto a la calificación de los hechos que en la misma se refieren como constitutivos de un delito de estafa del artículo 248.2 del CP, por la sencilla razón de que en dichos hechos no se describe manipulación informática o artificio semejante alguno, ocurre sólo que la tarjeta es utilizada por quien no es titular, que el comerciante conoce esa circunstancia y que quien usa la tarjeta firma los recibos de compra, es decir, no existen manipulaciones distintas a las que se realizan en los casos en que el comerciante desconoce que quien presenta la tarjeta no es titular de la misma.

Conclusiones

Bajo pena de incurrir en una interpretación extensiva, proscrita por el artículo 4.1 del vigente CP, la sustitución en una tarjeta de crédito o de débito originariamente legítima de los datos que vienen incorporados a su banda magnética por otros distintos no puede calificarse como una modalidad de la “fabricación” prevista en el número 1.º del párrafo primero del artículo 386 del CP, lo que, unido a la

supresión en el ámbito de los delitos de falsificación de moneda de la referencia a la alteración de moneda del artículo 283. 2.º del anterior CP, obliga a calificar aquel comportamiento como delito de falsificación de documento mercantil previsto en el artículo 392 en relación con el número 1.º del artículo 390.1, ambos del CP.

Sin embargo, considerando que la gravedad de la alteración que se ha descrito en la conclusión anterior es equivalente a la gravedad de la fabricación de tarjetas de crédito o de débito, es aconsejable de lege ferenda añadir en el párrafo primero del artículo 386 del CP la antigua referencia a la alteración de moneda legítima. En los casos de falsificación de tarjetas de crédito o de débito no es procedente la imposición de la pena de multa establecida en el párrafo primero del artículo 386 del CP, por cuanto que aquellas tarjetas carecen de valor aparente.

En general, la penalidad establecida en el 386.1 CP puede resultar excesiva o desproporcionada con la gravedad de determinadas conductas constitutivas del delito de falsificación de moneda, por lo que se entiende aconsejable flexibilizar dicha penalidad: bien mediante el establecimiento de un tipo básico (con una penalidad inferior a la actual) y de otro agravado; bien manteniendo la actual penalidad pero añadiendo la previsión de que, concurriendo determinadas circunstancias, haya de bajarse dicha penalidad.

La utilización de tarjetas de crédito o de débito, legítimas pero de otro titular o falsificadas, en establecimientos mercantiles o comercios constituye un delito de estafa del artículo 248.1 del CP y no un delito de robo con fuerza en las cosas de los artículos 237, 238.4.º y 239 del mismo CP, ni tampoco un delito de estafa informática del apartado 2 del citado artículo 248.

EMISIÓN, RETIRADA Y ENVÍO DE TARJETAS SIN SOLICITUD PREVIA DEL TITULAR

Ya hemos visto que para el Servicio de Reclamaciones del Banco de España que el hecho de que la entidad no pueda acreditar la previa solicitud del cliente, el envío discrecional de tarjetas basado en criterios comerciales es contrario a las buenas prácticas bancarias. En este sentido, el Código de Buena Conducta de la Banca Europea con respecto a los sistemas de pago mediante tarjeta, y en la CBE núm. 8/1990, establecen la obligatoriedad de entrega y posterior suscripción por el cliente en la emisión de medios de pago vinculados a las cuentas corrientes y de ahorro.

Del mismo modo, en la cláusula 8ª del Código de referencia se establece que el emisor de la tarjeta no puede entregar una tarjeta no solicitada a un cliente, salvo en caso de sustitución de otra.

Igualmente, la remisión por correo ordinario de documentos de trascendencia económica, como lo son las tarjetas bancarias y el PIN, no garantiza ni la certeza de su recepción por parte del destinatario, ni la constancia documental de que se ha efectuado la propia entrega.

SAP de Ciudad Real, de 28 de noviembre de 2007: no entregan el contrato

(...) No puede obviarse que en la misma forma de realizar el contrato a iniciativa exclusiva de la emisora sin más requisitos que se le proporcione un impreso diligenciado de datos por quien permanece ignorado para aquella en todo momento pues ni siquiera a posteriori existe comprobación al efecto, se incardina el riesgo que ello comporta, respecto cuya previsión es de tal evidencia que no puede ignorarse por una entidad tan notoria como lo es la del presente supuesto. Ese riesgo fácil de contemplar hipotéticamente se entiende asumido cuando se produce un uso irregular o fraudulento, como parece pudiera haber ocurrido aquí, aunque no se haya tomado iniciativa alguna para constatarlo y derivar de ese modo hacia el responsable el importe reclamado. En ese sentido, entrando en la carga probatoria que incumbía a la reclamante, a partir de que el demandado ha demostrado que el no firmó directa y personalmente la solicitud por no poder hacerlo dadas sus circunstancias personales (sordomudez y no saber escribir, ni firmar), también resultaba posible acreditar la identidad de la persona del uso de la tarjeta, al menos en lo que constituyó la adquisición del video con independencia de que se pagara su precio y no integre la petición que se hace en este juicio, así como la identidad de las disposiciones realizadas a través de las distintas oficinas bancarias que registran videográficamente tales operaciones. Actividad probatoria que se ha obviado. Pues, en definitiva, se trataría, al menos, de haber reducido las muy distintas posibilidades por las que se pudiera haber

efectuado la utilización de la tarjeta de crédito (familiares o personas del entorno del demandado que es jubilado y se halla en una Residencia, todos los que pueden conocer los requisitos pedidos en el formulario) y haber podido contar, en su caso, con datos indiciarios que permitieran la acogida de la demanda que, -no lo son el hecho mismos de haberse cargado los recibos anteriores dadas las circunstancias personales resaltadas,- por el contrario, atendiendo a lo dicho, no resulta viable.(...)”

INCORPORACIÓN DE CLÁUSULAS ABUSIVAS A LOS CONTRATOS: PRÁCTICA HABITUAL EN TARJETAS

Las entidades financieras, para eximirse de la responsabilidad en caso de uso indebido de la tarjeta, incluyen cláusulas abusivas en el contrato mencionando condiciones como: plazo de 24 horas para notificar la pérdida, robo o extravío y limita a 150 euros la responsabilidad del titular. Diversas sentencias han considerado estas cláusulas como abusivas, ya que notificarlo no es cuestión de tiempo, sino del momento preciso en el que se tiene constancia de la sustracción o extravío. Remitiéndonos al Código Civil en su art. 1.255 dice que “los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público”, disposición general que debe cumplir cualquier contrato lo que impide que existan cláusulas abusivas como la establecidas para el uso fraudulento con tarjetas.

SAP de Madrid, Sección 21ª, núm. 446/2007, de 18 de julio de 2007: no se puede limitar la responsabilidad

El demandante era titular de una tarjeta de crédito emitida por Caja España, asociada a una cuenta corriente de la que él era único titular. Se aporta el contrato de apertura de tarjeta de crédito de fecha 19-2-2001, (...). La cláusula 5ª sobre “Limitación de responsabilidad dice: el titular asume las responsabilidades derivadas de la utilización fraudulenta por terceras personas antes de la notificación prevista en el apartado b).3 de la cláusula 4ª. Esta responsabilidad queda limitada a un máximo de 25.000 Ptas. (150,25 €), siempre que la citada notificación se hubiera realizado antes de transcurridas las 24 horas del hecho que la motivó y siempre que no hubiera incurrido en dolo o negligencia grave. Sin perjuicio de otros supuestos, se entiende que concurre negligencia grave cuando la clave secreta está de tal modo unida a la Tarjeta que el robo o extravío de ésta conlleva el conocimiento de la misma”.

Procede confirmar la sentencia recurrida en cuanto a la declaración de nulidad del plazo de 24 horas que establece la cláusula 5ª del contrato de tarjeta de crédito, ya referido antes. Efectivamente dicha resolución parte de que no es contrario al equilibrio entre las posiciones de las partes la existencia de un reparto de responsabilidad entre ambas ni la limitación de responsabilidad contenida en la cláusula 5ª. Pero argumenta que si rompe ese equilibrio el plazo tan breve establecido, de manera que se cumplirá sólo de forma excepcional, perjudicando de manera desproporcionada al consumidor. Valoración que comparte plenamente esta Sala y que es sustentada por la resolución que menciona la Juzgadora “a quo”, Sentencia de la AP de Madrid, Sección 8ª, de 28-11-2003, la cual añade que “el desequilibrio en los derechos del consumidor en lo atinente a la condición general que nos ocupa, no negociada individualmente, al haber sido redactada previamente y no haber podido aquél influir en su contenido, emerge desde el momento en que el tan manido plazo de veinticuatro (horas) dificulta enormemente la posibilidad de resarcimiento y comporta un correlativo beneficio para la demandada que se verá exenta de indemnizar más que en las ocasiones en que la notificación se realiza en ese exiguo “lapsus temporal”, por lo que tiene carácter abusivo “por no atemperarse a las exigencias de la buena fe, ser desproporcionada, causar un notorio perjuicio al consumidor e implicar un desequilibrio claro en las obligaciones de las partes al respecto (...)”, en aplicación del art. 10.1 c),3 y art. 10 bis de la LGDCU, según la redacción dada por la D. Adicional Primera de la Ley sobre Condiciones Generales de la Contratación .

Transferencias bancarias: errores e incumplimiento de plazos, las razones más comunes en vía judicial

El contrato bancario de cuenta corriente es un contrato atípico a través del que se presta el servicio de caja, cuyos resultados se anotan contablemente por el sistema de cuenta corriente. El banco realiza pagos y cobros de la más variada índole, según las instrucciones del cliente y en función de la disponibilidad de fondos, y a falta de instrucciones precisas, actúa según las normas comunes de la buena práctica bancaria; lealtad, y beneficio de su cliente.

Dentro de los servicios bancarios vinculados a una cuenta corriente se encuentra la transferencia bancaria (operación multilateral donde intervienen diversos sujetos –ordenante, beneficiario, entidad de crédito). La relación que se establece entre el ordenante y la entidad financiera encaja dentro del contrato de comisión con lo que le serán aplicables las normas jurídicas de esta figura en cuanto a la determinación de la diligencia exigible y a la responsabilidad (SAP de Castellón de 24 de abril de 1997).

En lo que respecta al tema de la diligencia exigible a las entidades bancarias, es doctrina jurisprudencial, la que afirma que no es la de un buen padre de familia, sino la del comerciante experto que, normalmente, ejerce funciones de depósito y comisión (STS de 22 de septiembre de 2005; SSTs, de 15 de julio de 1988 y 9 de febrero de 1998). Por tanto, dado que es ella la que confecciona el sistema y dispone al caso de los medios personales y materiales, diseño y medidas de seguridad, y por ende en mayor disposición para corregir sus fallos, le corresponde probar que el cliente ha sido negligente o no ha tenido la diligencia exigible.

SAP de Alicante, Sección 9ª, núm. 136/2007, de 18 de abril: también hay problemas en el “envío de dinero”

“(…) la actuación de Foreign Exchange Company de España, SA, que gira bajo el nombre comercial de Western Unión, no estuvo revestida de la necesaria diligencia y buena práctica exigible a estas entidades dedicadas profesionalmente al servicio de envío de dinero. Dado que es esperable en su actuación un deber de lealtad, información y prevención como consecuencia de la cualificación profesional que ostenta y de la relación de confianza en que se sitúa el cliente frente a dicha entidad, de forma que le es exigible un modelo de diligencia profesional –cabalmente empresarial– al que se imputabiliza todo daño proveniente de culpa leve o de negligencia en el desempeño del cargo.

STS de 10 de julio de 2003: negligencia de bancos y cajas al cumplir la orden de transferencia

“Es, pues, una medida que atiende a un criterio objetivo y abstracto, exigible según las circunstancias es la diligencia que dentro de la vida social puede ser exigida en la situación concreta a persona razonable y sensata correspondiente al sector del tráfico o de la vida social cualificados por la clase de actividad a enjuiciar. Según este criterio objetivo, ha de resolverse la cuestión de si el agente ha obrado con el cuidado, atención o perseverancia exigibles, con la reflexión necesaria y el sacrificio de tiempo precisos. Al respecto no es pues decisivo la individualidad del agente, sino las circunstancias que determinarán la medida necesaria de diligencia y cautela.”

Las transferencias se tramitan de acuerdo con las normas reguladoras del Sistema Nacional de Compensación Electrónica, en función de las directrices del ordenante. La orden de transferencia, en cumplimiento de lo estipulado contractualmente, obliga al banco no sólo a su simple ejecución, sino a asegurar su bien fin. Por tanto, dicha ejecución será la que determine el nivel de diligencia empleada por la entidad en cada caso concreto (la SAP de Vizcaya de 18 de enero de 2000. Establece la negligencia del banco al ejecutar igualmente la orden de transferencia, cuando ya había sido revocada previamente por su cliente.). Desde el punto de vista procesal, el resañado deber de diligencia implica que aún en el caso de que la demanda se interpusiese exclusivamente frente a la entidad financiera, no sería un supuesto de litisconsorcio pasivo necesario.

Por último, como ejemplos de negligencia por parte de la entidad en relación a la correcta ejecución

de la orden pueden enumerarse los siguientes: ejecución de la orden de transferencia sin verificar la identidad del ordenante (STS de 15 de julio de 1988, RJ 1988/5717); realización de la transferencia a una cuenta diferente de la del destinatario (STS de 14 de noviembre de 1987, RJ 1987/9987); repetición de una misma transferencia (SAP de Valencia, Sección 8ª, de 15 de junio de 1999); realización de la transferencia cuya orden se ha dado por teléfono a favor de una persona distinta al titular de la cuenta, sin comprobar la veracidad de la firma en la confirmación escrita de la instrucción (SAP de Málaga, Sección 5ª, de 14 de febrero de 2001).

SENTENCIA DE LA A.P. DE VALENCIA (SECCIÓN 8.ª), DE 15 DE JUNIO DE 1999:

ERROR DE LA ENTIDAD EN LA EJECUCIÓN DE UNA ORDEN DE TRANSFERENCIA

Supuesto de hecho

Por la entidad demandante Banco E. de C., S.A., se formuló demanda contra D. Rafael F.M., en reclamación de la cantidad de 2.033.471 ptas., alegando, en base a su pretensión, que recibió una orden de parte de su cliente, la mercantil C., S.A., de realizar una transferencia por importe de 2.033.471 ptas. a favor del demandado y hoy recurrente D. Rafael F.M., lo que así realizó el día 22 de julio de 1994, recibiendo el demandado dicha cantidad.

Sin embargo, y debido a un error por parte de la oficina bancaria, se duplicó la transferencia, recibiendo el demandado poco tiempo después nuevamente la referida cantidad de 2.033.471 ptas.

Al darse cuenta del error sufrido la entidad bancaria actora reclamó del demandado el importe de la segunda transferencia a lo que éste hizo caso omiso.

La sentencia de instancia estimó íntegramente la demanda y contra la misma recurre en apelación D. Rafael F.M., solicitando la revocación de la misma y en consecuencia se desestime la demanda, alegando que la mercantil ordenante de la transferencia C., S.A., le adeudaba la cantidad que recibió, por lo que no concurren los requisitos legales necesarios para exigirle la devolución de la cantidad reclamada en demanda.

La transferencia bancaria

La transferencia es una operación bancaria mediante la cual el cliente de una entidad (ordenante) ordena a ésta que con cargo a su cuenta transfiera una determinada suma a otra cuenta, del mismo o de distinto titular (beneficiario), situada en la misma entidad o en otra distinta. Lo que caracteriza a la transferencia es que el movimiento de fondos se efectúa sin la utilización de efectivo o numerario, mediante un simple juego de escrituras: adeudo de la cuenta del ordenante y abono de la del beneficiario. De ahí que se afirme que la transferencia bancaria conlleva una operación contable.

Naturaleza jurídica de la transferencia

En opinión de la doctrina, las relaciones del ordenante con su banco participan de la naturaleza del mandato. La calificación de estas relaciones como de mandato deriva de la conceptualización de la transferencia bancaria como una operación que se desarrolla en el marco de un contrato de cuenta corriente o de cuenta de ahorro a la vista, contratos que son reconducibles al mandato. Aunque en la Sentencia no se dice expresamente que exista una relación de cuenta bancaria entre el ordenante (la mercantil C., S.A.) y su banco (Banco E. de C., S.A.) presumimos que se da dicha relación, ya que es lo más habitual.

La orden de transferencia

Las operaciones que lleva a cabo el banco en la ejecución del servicio de caja requieren un impulso o declaración de voluntad de sus clientes que ponga en marcha la operación, siendo frecuente en el lenguaje bancario el empleo del término orden para hacer referencia a estas manifestaciones de voluntad.

Cuando se trata de una transferencia, el acto del ordenante que pone en marcha esta operación se denomina orden de transferencia. Mediante la emisión de la orden el cliente-ordenante ordena a su banco que transfiera una determinada cantidad al beneficiario, facultándole para adeudar su cuenta.

Cumple así la orden de transferencia una doble función: sirve como autorización al banco para adeudar la cuenta del ordenante y como orden de transferir los fondos al beneficiario.

La orden de transferencia funciona como causa de la operación, es decir, como causa de la remisión de fondos al beneficiario. En consecuencia, la atribución de fondos que el Banco E. de C., S.A., realiza a favor de D. Rafael F.M. debe obedecer a la existencia de una orden de transferencia de la mercantil C., S.A. al Banco E. de C., S.A. Sin orden de transferencia la posible atribución de fondos al beneficiario (cuestión sobre la que nos detendremos más adelante) carecería de causa y, por tanto, de validez.

El error del banco en la ejecución de la orden de transferencia

En la ejecución de una orden de transferencia pueden producirse errores cometidos bien por el ordenante bien por los bancos que intervienen en la operación (banco del ordenante, bancos intermediarios o banco del beneficiario).

El error puede producirse en la identificación del beneficiario (se identifica al beneficiario solamente por el número de cuenta y éste es erróneo) o en la cuantía del importe que ha de transferirse (se desean transferir 100.000 pesetas y en su lugar se indica 1.000.000 de pesetas o 10.000 pesetas). El error puede consistir en la emisión de un duplicado erróneo de la orden de transferencia (se envía dos veces la misma orden) o en la existencia de discrepancias en los datos consignados (se identifica al beneficiario por el número de cuenta y por el nombre y ambos no coinciden, o se indica el importe de la transferencia en letras y en números y existe una contradicción entre ellos), etc.

En el caso que nos ocupa nos encontramos ante un error del banco (Banco E. de C., S.A.), error que consiste en la emisión de un duplicado erróneo. Como consecuencia de la ejecución de ese duplicado erróneo, el beneficiario de la primera orden de transferencia (Rafael F.M.)—que si era correcta—recibe por segunda vez en su cuenta el importe de esa primera orden de transferencia. La cuestión central es si el beneficiario puede retener los fondos correspondientes a la segunda orden de transferencia (el duplicado erróneo) alegando que, a pesar del error, esa cantidad le era debida por el ordenante (la mercantil C., S.A.).

En el caso de que la cantidad no le fuera debida, la doctrina coincide en afirmar que el banco puede repetir contra el beneficiario alegando cobro de lo indebido (arts. 1895 y ss. CC), aunque el banco soporta siempre el riesgo de que el beneficiario no pueda restituir los fondos, por ejemplo, porque sea insolvente.

No hay acuerdo entre los autores cuando como consecuencia del error el beneficiario recibe en su cuenta una cantidad que el ordenante le debía. Hay quien opina que en este caso el banco no puede reclamar la restitución de los fondos al beneficiario alegando cobro de lo indebido; el beneficiario estaría, por tanto, legitimado para retener los fondos. Se produciría un pago por cuenta de tercero (el banco paga al beneficiario por cuenta del ordenante), pudiendo el banco que cometió el error reclamar al ordenante la cantidad entregada al beneficiario. Trasladando esta opinión a los hechos que son objeto de la Sentencia, D. Rafael F.M. estaría legitimado para retener los fondos en su poder y la deuda que mediaba entre él y la mercantil C., S.A. quedaría saldada: el Banco E. de C., S.A. habría pagado por cuenta de la mercantil C., S.A. y, lógicamente, aquél podrá reclamar a ésta el importe de la deuda (claro está que el Banco E. de C., S.A. soporta en este caso el riesgo de que la mercantil C., S.A. no pueda pagarle porque sea insolvente).

Hay quien, por el contrario, entiende que la solución ha de ser la misma en ambos casos; es decir,

que tanto si la cantidad es debida al beneficiario como si no, el banco que comete el error puede repetir del beneficiario alegando cobro de lo indebido. En este sentido se ha afirmado que no puede olvidarse que hay un error, es decir, que el banco actúa pensando que está cumpliendo un mandato o instrucción que en realidad no existe. En consecuencia, el abono realizado en la cuenta del beneficiario no trae causa de la voluntad del ordenante, sino de la voluntad errónea del banco. Por ello, el beneficiario se convierte frente al banco en acreedor de una cantidad que no tenía “derecho a cobrar” y que por error le ha sido “indebidamente entregada” (art. 1895 CC).

A esta última conclusión, llega la Sentencia de la Audiencia Provincial de Valencia. En efecto, en sus fundamentos de derecho se afirma que “concurren todos los requisitos exigidos para que pueda prosperar la acción de repetición basada en el cobro de lo indebido” ya que el banco realizó un pago “con la intención de extinguir la deuda, cuando ya no existía la obligación, pues ésta había sido ya pagada” [el artículo 1901 del CC dispone que “Se presume que hubo error en el pago cuando se entregó cosa que nunca se debió o que ya estaba pagada...”].

Se dice, además, que el beneficiario no puede alegar en ese proceso que el ordenante le debía la cantidad erróneamente abonada en su cuenta, “por lo que si el demandado estima que la mercantil C., S.A., le adeudaba dicha cantidad deberá ejercitar la oportuna acción de reclamación de cantidad en otro proceso pero no en este en el que no es parte dicha sociedad”.

En nuestra opinión, la solución a la que llega la Audiencia Provincial de Valencia es correcta (es decir, el banco está legitimado para reclamar al beneficiario el importe de la segunda orden de transferencia), pero no así la argumentación que ofrece. El error estriba en considerar que entre el banco y el beneficiario puede darse una relación jurídica por cobro de lo indebido (en los fundamentos de derecho se dice expresamente que “la relación jurídica por el cobro de lo indebido se constituye, en este caso, entre el Banco demandante y el demandado D. Rafael F.”) cuando, en realidad, dicha relación (o su opuesta, el cobro de lo debido) sólo puede establecerse entre el ordenante y el beneficiario. En efecto, quien debe o no una cantidad al beneficiario es el ordenante, no el banco y, en consecuencia, para saber si existe o no cobro de lo indebido habrá que investigar si el ordenante debía o no la cantidad en cuestión al beneficiario.

Es más, puede afirmarse que acudir a la institución del cobro de lo indebido sólo tiene sentido cuando el error es del ordenante, pero que no puede acudirse a esta figura cuando el error es de la entidad bancaria. En efecto, si el error del ordenante hace que el beneficiario reciba unos fondos que no se le debían, el ordenante podrá repetir de él alegando cobro de lo indebido. Si, por el contrario, la cantidad le era realmente debida, el ordenante no podrá reclamarla y se producen los efectos del pago (el acreedor queda satisfecho y el deudor liberado de su deuda).

Si el error procede del banco, la solución no se encuentra en la institución del cobro de lo indebido (es decir, no hay que averiguar si existe o no un cobro de lo indebido), sino en la propia operativa de la figura de la transferencia. Señalamos más arriba que la remisión de fondos efectuada a favor del beneficiario debe obedecer a la existencia de una orden de transferencia. Cuando existe dicha orden, la atribución de fondos realizada al beneficiario tiene una causa, que es la orden de transferencia. Cuando falta esa orden la atribución de fondos efectuada al beneficiario carece de causa y, en consecuencia, no sería válida. No cabe, pues, plantearse si el ordenante debía o no al beneficiario la cantidad erróneamente transferida. Siempre y en todo caso el banco podrá reclamar del beneficiario la cantidad indebidamente abonada en su cuenta alegando que la remisión de fondos efectuada a su favor carece de causa por no existir orden de transferencia.

SENTENCIA DEL TRIBUNAL SUPREMO 236/2009, DE 14 DE ABRIL:

LA ENTIDAD BANCARIA RESPONDE POR LA DISTRACCIÓN DE FONDOS DE UNA CUENTA CORRIENTE SIN CONSENTIMIENTO NI AUTORIZACIÓN DE SUS TITULARES

Supuesto de hecho de la sentencia

El objeto del proceso versa sobre la distracción de fondos de una cuenta corriente en la que se hicieron cargos y extracciones de dinero no autorizadas y sin conocimiento de los titulares, lo que se llevó a cabo por empleados de la entidad y por una persona colaborador remunerado del Banco que era gerente de una empresa de los citados titulares pero no estaba autorizado para disponer en la cuenta corriente particular, y aprovechó la relación de confianza expresada para, mediante una información falsa, evitar que los cuentacorrentistas se enteraran del uso que se hacía de sus depósitos.

Procedimiento judicial de la demanda

A raíz de esta circunstancia se interpuso demanda de juicio ordinario de menor cuantía ante el Juzgado de Primera Instancia, quien en su fallo condenó a dicha entidad a la rendición de cuentas detalladas y documentadas de todos los asientos conocidos por los titulares y al abono del saldo que resulten acreedores más los intereses legales y moratorios.

Este fallo fue la Audiencia Provincial de Bilbao, ante la que se interpuso recurso de apelación por parte de la entidad, reduciendo la cantidad a abonar al límite máximo del juicio de menor cuantía, y concretando que los intereses de demora surgen desde el requerimiento notarial a la entidad bancaria para que proceda a la rendición de cuentas.

Como consecuencia del ello, se plantea ante la Sala Primera, de lo Civil, del Tribunal Supremo recurso de casación y recurso de casación por infracción procesal.

El fallo de este recurso de casación finalmente reconoce que la cuantía que corresponde abonar por la entidad condenada es la inicialmente reclamada por aquellos titulares, dado que al tratarse de la reclamación de una cuantía indeterminada por ignorarse el saldo total de la suma defraudada, la ley prevé el trámite del juicio de menor cuantía, sin que ello implique conformidad con la suma máxima de dicho trámite.

Y en lo relativo al recurso de casación, presentado por la entidad bancaria, en su fallo se reconoce que los intereses moratorios, en lugar de devengarse desde el requerimiento de rendición de cuentas, deben comenzar a raíz de la presentación de la demanda, dado que con aquel requerimiento no hubo ninguna interpelación sino una mera petición. Este fallo condena a la entidad en concreto al pago de 160 millones de las antiguas pesetas más intereses y costas.

ADEUDO DE RECIBOS NO DOMICILIADOS

Constituye una práctica moderna que la banca ha implantado en aras a una mayor agilidad operativa y, en definitiva, en beneficio propio, el adeudo indiscriminado de recibos, sin que medie en poder de la entidad la orden previa de domiciliación que cuente con un código correcto de cuenta corriente del cliente.

En estos casos, la entidad ha de poner en conocimiento del titular de la cuenta, a la mayor brevedad posible, los adeudos practicados para que puedan decidir sobre cuáles atender y cuáles no.

SAP de Sevilla, Sección 2ª, núm. 254/2005, de 6 de junio de 2005: el banco no debe atender ordenes de pago no autorizadas por el usuario

“Los extractos de los movimientos bancarios revelan que Banco Popular y Dª Carmela están vinculados por contrato bancario de apertura de cuenta corriente, y, aunque el concreto documento contractual no haya sido aportado a las actuaciones, es obvio que en su clausulado no debe figurar ninguna estipulación que faculte al Banco a atender, por cuenta de la cliente, recibos no emitidos a su nombre, u órdenes de pago no autorizadas por la cuentacorrentista.

En la orden de domiciliación bancaria de recibos por servicios telefónicos, obrante al folio 7, se indica con toda claridad cuál es el número de teléfono cuya facturación debía ser atendida en el Banco Popular por cuenta de la Sra. Carmela.

Los cargos efectuados en la cuenta corriente de la actora correspondientes al núm. NUM000 (y referenciados bajo la cifra NUM001) son incorrectos, pues la orden de domiciliación únicamente comprendía las facturas relativas al núm. de teléfono NUM002; el Banco, incumpliendo la obligación de custodiar diligentemente el dinero depositado a través del contrato de apertura de cuenta corriente, efectuó entre los años 1997 y 2002 pagos de facturas para los que carecía de la pertinente autorización.

No existiendo correspondencia entre orden de abono de recibos de Telefónica y cargos efectuados en la cuenta corriente, la entidad bancaria, que no estaba autorizada para cargar en la cuenta de la cliente recibos del Teléfono núm. NUM003, debe responder por cumplimiento irregular o defectuoso imputable a culpa contractual, al amparo del art. 1101 del Código Civil.”

Cheques: la falsedad lo más habitual

STS, Sala 2ª, de lo Penal, núm. 1195/2005, de 9 de octubre de 2005

El daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques, o hubiere procedido con culpa. la falsificación de un cheque y su utilización posterior por el autor de la falsificación para cometer una estafa, debe sancionarse como concurso de delitos entre estafa agravada y falsedad en documento mercantil.

SAP de Madrid, Sección 21ª, núm. 463/2006, de 27 de octubre de

El daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques o hubiera procedido por culpa, existiendo pues una cierta responsabilidad objetiva ex lege de la entidad financiera librada, en tanto que solo está autorizada al pago de los cheques emitidos por el librador.

STS Sala 1ª, de lo Civil, de 18 de julio de 1994

“El art. 156 de la Ley Cambiaría y del Cheque (en que se base la acción ejercitada), viene a tipificar un específico supuesto de responsabilidad por culpa contractual, el expresado motivo ha de ser desestimado, ya que si la responsabilidad indemnizatoria que, conforme al inciso primero del citado precepto, corresponde al banco librado por el daño que resulte del pago de un cheque falsificado, puede quedar totalmente excluida o eliminada cuando el titular de la cuenta corriente (“el librador”, según la dicción legal), haya sido negligente en la custodia del talonario de cheques o hubiere procedido con culpa (incisos segundo y tercero del mismo precepto), resulta indudable que, cuando, existiendo negligencia por parte del banco librado, concurra también una evidente conducta culposa del perjudicado titular de la cuenta corriente (“librador”), cuya concurrencia culposa, como en todos los casos de responsabilidad por culpa contractual o extracontractual, es incluso apreciable de oficio (Sentencias de esta Sala de 18 de octubre de 1982, 22 de abril de 1987, 7 de junio de 1991, entre otras), resulta indudable, decimos, que en dicho supuesto los Tribunales deben moderar la responsabilidad del agente y reducir en proporción su deber de indemnización, repartiendo el daño con el perjudicado.

Cuando no fuese posible presentar el cheque, levantar el protesto, o hacer las declaraciones equivalentes dentro de los plazos fijados, por causa de fuerza mayor, se entenderán prorrogados dichos plazos.”

Phishing: una nueva forma de fraude que ya tiene respuesta de los Tribunales

El phishing es un delito mediante el cual los delincuentes usurpan las claves de acceso a las cuentas bancarias de un titular con el objeto de robarle su dinero. Este tipo de hechos delictivos ha prolifera-

do cuantitativamente en los últimos años. Además, las bandas organizadas cada vez emplean unos medios técnicos más modernos y complejos que dificultan más si cabe su detención. el evitar ser una víctima de estos fraudes.

Frente a esto, surge otro problema de igual envergadura para los usuarios de las entidades financieras: las cláusulas de exoneración de responsabilidad que dichas entidades incluyen en los contratos (contratos tipo o de adhesión). Es decir, en caso de que el consumidor sea víctima de este fraude, tendrá que asumir el perjuicio económico.

Una sentencia ganada por ADICAE

“(...) como dice la SAP de Madrid, Sección 13ª, de 11 de febrero de 2005 las referidas cláusulas desplazan la responsabilidad que incumbe al Banco hacia su cliente que no ha tenido ninguna participación en el daño causado, infringiendo así lo contemplado en la cláusula 14 de la Disposición Adicional primera de la Ley General para la Defensa de Consumidores y Usuarios en cuanto impone limitación de los derechos del consumidor.” (Jdo. de 1ª Instancia nº 2, de Castellón, núm. 126/2008, de 25 de junio de 2008. Fdto. Jco. 6º, sentencia favorable para el consumidor obtenida por ADICAE).

En este sentido supone un gran avance y un importante logro para ADICAE en la defensa y protección de los derechos de los consumidores y usuarios de servicios de banca electrónica la sentencia del Juzgado de 1ª Instancia nº 2 de Castellón, núm. 126/2008, de 25 de junio de 2008. Dicha resolución falla a favor de los clientes indicando que la entidad tiene la obligación de suministrar a sus clientes una información clara y precisa sobre las recomendaciones de seguridad que debe emplear cada vez que accede al servicio de banca electrónica.

En la Estipulación General IV, de dicho contrato se dice que “Caja de Ahorros B.” queda exonerada de toda responsabilidad debida a las deficiencias o fallos de seguridad en las redes de comunicación, tales como virus informáticos o debidos a la utilización por los usuarios o autorizados de un navegador deficiente o mal configurado. Asimismo, “Caja de Ahorros B.” no responderá de los daños que se puedan causar por la intromisión ilegítima de terceros en sus sistemas.

Fto. Jco. 6º: (...) no es dado imponer al consumidor la renuncia indiscriminada al derecho que le pueda asistir para reclamar, frente a la entidad que le proporciona los medios técnicos necesarios para una mejor o más cómoda prestación de sus servicios, en aquellos supuestos en los que, no mereciendo la consideración de caso fortuito o fuerza mayor así como los efectivamente no imputables a la propia entidad bancaria, le ocasionen daños y/o perjuicios.

No previno ni informó adecuadamente al consumidor

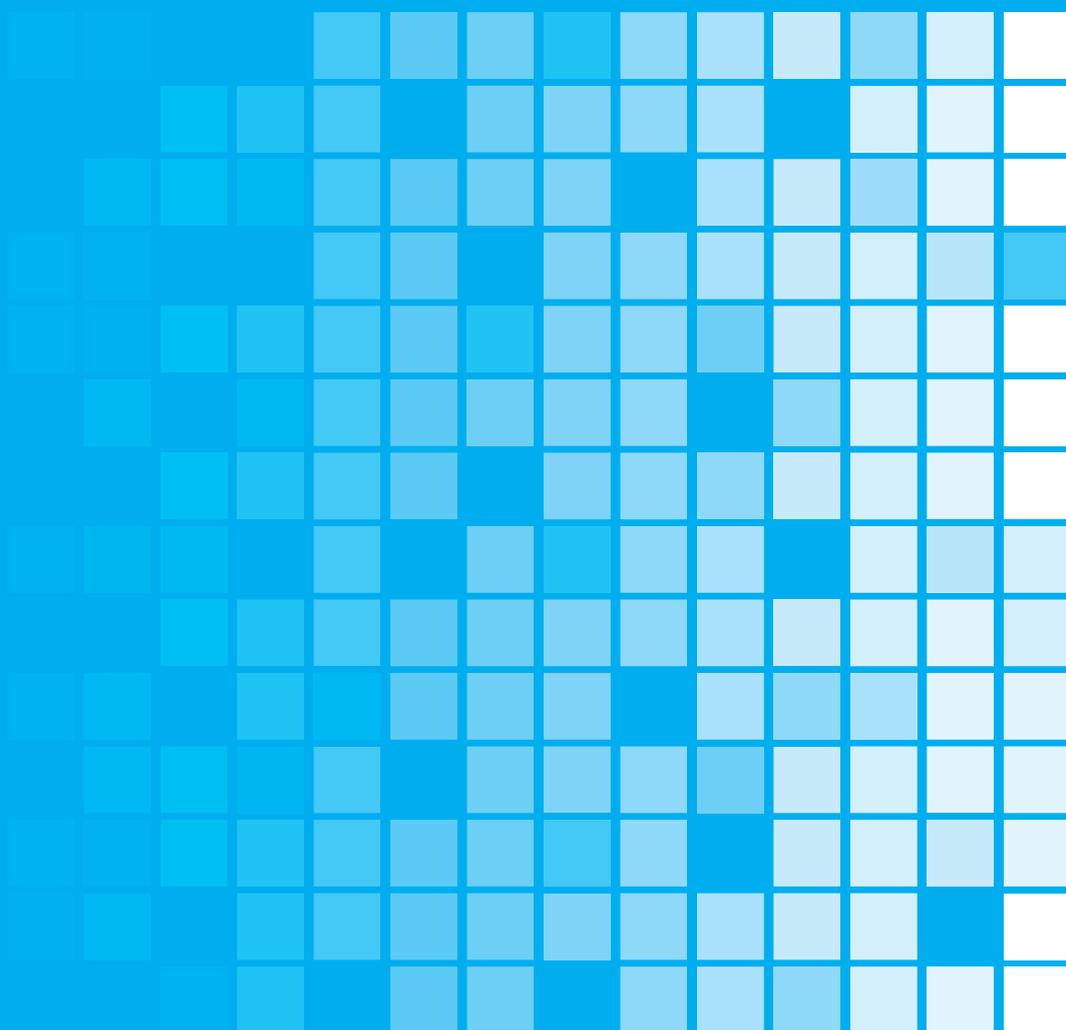
*Enlazando con cuanto acaba de exponerse, no puede desconocerse la conclusión a la que llegó el Servicio de Reclamaciones del Banco de España en informe de fecha 23 de noviembre de 2006 ... ante la reclamación presentada por los ahora demandantes por los mismos hechos que posteriormente han sido objeto del presente pleito civil. Tal como expone el Banco de España en la segunda consideración jurídica de su escrito, revisada la documentación aportada al expediente, entre la que figura el contrato de servicios de banca electrónica , en fecha 14 de noviembre de 2005, identificado con el número 1486296, no se desprende que **la Caja hubiera facilitado a su cliente las advertencias necesarias para evitar el fraude en el comercio electrónico con anterioridad a que se produjeran las controvertidas transferencias.***

Y si bien es cierto que ese Servicio no tiene competencia para determinar las consecuencias que de los pactos, cláusulas y condiciones establecidos en el ámbito de las relaciones regidas por normas de derecho privado puedan derivarse, ya que es competencia exclusiva de los tribunales de justicia la resolución de las discrepancias que puedan producirse de las relaciones mercantiles entre las partes, pero sí es un dato más a tener en cuenta en esta jurisdicción civil (donde ahora se han planteado cuestiones concernientes a las relaciones contractuales entre las partes) el hecho de que dicho organismo, tras examinar la documentación aportada al expediente por las partes, no haya podido constatar que la entidad hubiera ofrecido a su cliente una información clara y precisa sobre las recomendaciones de seguridad que debe emplear cada vez que accede al uso de la línea electrónica .

Así pues, el Servicio de Reclamaciones del Banco de España deja claro el alcance de su escrito y, sin lugar a dudas, lo informado por aquél no vincula a las partes de este proceso civil, pero considera este Juzgador que sí debe tenerse presente la opinión autorizada de los técnicos componentes de mentado Servicio respecto al comportamiento de “Caja de Ahorros B.” respecto de la información y recomendaciones de seguridad a sus clientes, en la banca electrónica .

Anexo II

Normativa sobre fraude en medios de pago en países partners



Frente a los fraudes en medios de pago, la normativa de los distintos países europeos necesita cohesión



Rumania

El fraude en medios de pago en la legislación rumana

La normativa rumana recoge en su código civil los requisitos que deben cumplir las entidades bancarias para asegurar la correcta información del consumidor en la contratación de servicios financieros, pero en la práctica, muchos bancos y cajas no cumplen estos requisitos.

1. MARCO LEGISLATIVO GENERAL

LA PROTECCIÓN DE LOS CONSUMIDORES EN LA NORMATIVA CONSTITUCIONAL

A pesar de que las leyes fundamentales rumanas no contienen disposiciones especiales sobre protección del consumidor, existen algunos artículos constitucionales que hacen referencia a la protección al ciudadano en general, como consumidor.

Por ejemplo, en el artículo número 135. 2, letra a) de la Constitución adoptada en 1991 y revisada en el 2003 se estipula que el Estado debe asegurar "un comercio libre, protección a la competencia limpia, aprovisionamiento de un marco favorable para estimular y sacar provecho de cada factor de producción". Esta disposición se refiere principalmente a fomentar el comercio y la competencia sin mencionar expresamente la protección al consumidor. No obstante, todos sabemos de la coexistencia que existe entre el libre comercio, la competencia limpia y la protección de los derechos de los consumidores, quienes son beneficiarios directos de las actividades de protección.

El artículo 17 también estipula que "El Estado estará obligado a tomar medidas de desarrollo económico y protección social, de forma que asegure un estándar de vida decente para sus ciudadanos". Es obvio que este tipo de medidas incluyen la protección de los intereses sociales y económicos del ciudadano. Solamente se puede asegurar un estándar de vida decente defendiendo sus intereses como consumidores.

Una disposición importante mencionada en el artículo 21 es la que se refiere a los ciudadanos considerados como consumidores: "Cada individuo tiene derecho a llevar casos a los tribunales para la defensa de los derechos legítimos, libertades e intereses". Esta afirmación garantiza el libre acceso a la justicia, que es un derecho fundamental y una condición imperativa de la eficiencia jurídica.

LOS DERECHOS Y LIBERTADES FUNDAMENTALES EN LA CONSTITUCIÓN

Los principios esenciales que fundamentan la mayoría de los derechos de los consumidores importantes son los que se mencionan en el Capítulo II titulado "Derechos y libertades fundamentales".

Por ejemplo, en el artículo 22 se garantiza el derecho a la vida y a la integridad física y mental. Estas estipulaciones necesitan ser corroboradas con el artículo 5 de las Normas de Consumo que mencionan la obligación del Estado de asegurar "la protección del consumidor contra riesgo de consumir un producto o servicio que pueda ser perjudicial para su vida, salud, seguridad o que pueda afectar a sus derechos e intereses legítimos".

Otros principios que se mencionan en el mismo capítulo que pueden estar relacionados con los derechos de los consumidores son: el derecho a la defensa, el derecho a la información, el derecho a la protección de salud, el derecho a un medio saludable, el derecho de asociación, el derecho a la propiedad privada y el derecho de demanda. Todos estos derechos del ciudadano fundamentales también se encuentran en la legislación específica sobre protección al consu-

midor. El ejercicio de estos derechos constitucionales sólo puede ser limitado por ley, en condiciones especiales de necesidad y adecuación.

Todas estas prerrogativas fundamentales mencionadas en la Constitución Rumana están fuertemente relacionadas con los derechos del consumidor y se benefician de una aplicación eficiente si están internacionalmente reconocidas, a través de convenciones, tratados o acuerdos internacionales. Una prioridad de cualquier estado es el reconocimiento, garantía y defensa de los derechos y libertades fundamentales del ciudadano (incluyendo los de protección al consumidor).

Considerando esta atribución y la coexistencia necesaria entre los derechos y las libertades generales de los ciudadanos y los intereses especiales de los consumidores, es importante hacer mención a la Resolución número 403/28.10.2003 tomada por el Tribunal Constitucional en cuanto a la excepción de disposiciones inconstitucionales del artículo 14, apartado 1 y artículo 15, apartado 1, 2 y 4 de la OG 21/1992.

Para rechazar esta excepción, el Tribunal Constitucional mencionó lo siguiente: "Las obligaciones del comerciante a cambiar el producto o devolver el dinero es una obligación general y está condicionada por la petición de esto, por la existencia de alguna deficiencia en la calidad o funcionamiento del producto. Esta petición del consumidor no da lugar a una obligación alcanzable y forzada. El comerciante puede llevar a cabo la petición del consumidor, pero si considera que su petición es injusta tiene derecho a rechazarla. En esta situación no sólo los intereses del consumidor reclaman justicia, el comerciante también tiene interés en probar su versión, usando los medios legales de prueba. De esta forma, los textos de leyes estudiados no restringen a nadie el derecho a la justicia, no limita el derecho a la defensa y no contienen ninguna disposición discriminatoria".

Como conclusión, la legislación en cuanto a la protección de los consumidores no contradice al derecho constitucional del libre acceso a la justicia, el derecho a la defensa o indiscriminación aunque tiene un carácter protector obvio a favor de los consumidores.

LA NORMATIVA DE LOS MEDIOS DE PAGO SEGÚN EL CÓDIGO CIVIL

Las disposiciones legales especiales que regulan la protección de los consumidores se completan con el derecho común, especialmente con las disposiciones recogidas en el Código Civil.

Inspirado en el Código Civil francés, el romano contiene en el Libro III, Título III disposiciones que regulan los contratos. Entre estos, están estas estipulaciones que hacen referencia a las condiciones necesarias y esenciales para validar un acuerdo. El no cumplimiento de estas condiciones conduce a la nulidad del contrato.

Para validar un contrato (también para los contratos donde una de las partes es un consumidor), la aprobación debe cumplir ciertas condiciones: que venga de una persona con juicio (con capacidad para contratar); que se exprese con la intención de producir efectos jurídicos; que se exteriorice y sea válido (que no sea modificado por algún vicio de consentimiento).

Según el artículo 953 del Código Civil, "el consentimiento no es válido cuando es dado por error, bajo violencia o sorprendido por dolo".

EL ERROR COMO VICIO DEL CONSENTIMIENTO

La definición de error es la falsa representación de la realidad en el momento de confirmar un acuerdo. El vicio de consentimiento tiene tres formas:

El error-obstáculo, puede aparecer cuando el consumidor estaba equivocado sobre la naturaleza del documento jurídico (error in negotio) o cuando el consumidor estaba equivocado sobre la naturaleza del objeto (error in corpore). La sanción es la nulidad absoluta del acuerdo. Es muy difícil probar este tipo de error.

El error-vice de consentimiento significa la falsa representación en cuanto a las cualidades substanciales del objeto (error in substantiam) o la parte (error in personam). Este tipo de error es sancionado con la nulidad relativa, pero es muy difícil conseguir probarlo.

El error indiferente ocurre cuando la falsa representación contempla circunstancias menos importantes que no afectan a la validez del contrato.

La acción para invalidar un contrato formado por un consumidor por riesgos de error tiene que ser rechazado por el tribunal de ley por no poderse demostrar, o por considerarlo inexplicable ya que el consumidor debía haber sido informado.

LA VIOLENCIA EN LA CONTRATACIÓN

La violencia consiste en amenazar a una persona con un fin perjudicial para que tenga temor, lo que lo hace determinar cerrar un acuerdo que de otra manera nunca habría cerrado.

La violencia puede ser:

Física: la amenaza contempla la integridad física de la persona o de sus bienes. Este tipo de violencia es difícilmente demostrable en la relación entre un profesional y un consumidor.

Moral: la amenaza se refiere al honor, credibilidad o sentimientos del individuo.

En acuerdos donde el consumidor es una de las partes no puede haber una forma de violencia económica, un tipo de abuso del poder practicado por los profesionales para que el consumidor cierre el contrato. Esta es una forma menos visible de violencia y es prácticamente imposible de probar.

EL DOLO EN LOS ACUERDOS CON EL CONSUMIDOR

El dolo consiste en engañar a una persona astutamente para conseguir que otra persona cierre un acuerdo. Este tipo de vicio es clasificado en:

Dolo principal: el error contempla elementos importantes del acto jurídico. La sanción es la invalidación del contrato.

Dolo incidente: el error contempla circunstancias menos importantes para la validez del contrato.

OTROS VICIOS DEL CONSENTIMIENTO

Otro tipo de vicio de consentimiento es la lesión, aunque el Código Civil solamente concede a los menores la posibilidad de apelar a este tipo de vicio. La lesión consiste en la mayor desproporción entre las prestaciones de las partes. Las cláusulas abusivas quizás crean una falta de equilibrio económico en la desventaja del consumidor.

EL CONSENTIMIENTO LIBRE DEL CONSUMIDOR Y SU SITUACIÓN DE INFERIORIDAD

El consumidor debe expresar un consentimiento libre y no viciado cuando cierra un contrato, aunque en la mayoría de los casos esté en una situación de inferioridad económica que los profesionales conocen.

En caso de que su voluntad fuese alterada por cualquier vicio de consentimiento, el contrato ilegal debe ser cancelado para proteger los intereses del consumidor. La sanción en este caso es la total nulidad del contrato que en algunas situaciones puede estar en detrimento del consumidor.

Además, es muy difícil demostrar el vicio de consentimiento por la parte que lo afirma. Aunque la tendencia de la práctica jurídica es fomentar y facilitar la misión del demandante, la tarea de demostración no se rechaza en las los litigios entre los profesionales y los consumidores. La deshonestidad del profesional no es presunta, el consumidor tiene que probarla. Por estas razones, se prefiere invalidar las cláusulas abusivas sobre los vicios de consentimiento, menos usadas en la cuestión de protección del consumidor.

2. OTRA LEGISLACIÓN SOBRE LA MATERÍA

Otra de la normativa que tenemos que tener en cuenta ya que en alguna medida puede afectar a los derechos del consumidor es la que a continuación enumeramos:

La Ley 365/2002 modificada por la Ley 121/2006 que contempla el comercio electrónico.

La Resolución del Gobierno número 1308/2002 de aprobar las normas metodológicas considerando el comercio electrónico.

La Ley 677/2001 para la protección de individuos considerando el uso de información personal.

Orden número 52/2002 que contempla la aprobación de los requisitos de seguridad mínimos para el uso de información personal.

Ley número 455/2001 que contempla la firma electrónica.

La Resolución del Gobierno número 7/2004 que contempla la protección jurídica de servicios basados en el acceso condicionado.

Normativa 4/2000 del Banco Nacional de Rumanía que contempla los medios de pago a distancia.

3. LAS PARTICULARIDADES EN LA LEY APLICABLE

Los profesionales, de acuerdo con su campo de actividad, deben asegurar una información completa, correcta y precisa sobre las características esenciales de los productos y servicios facilitados a los consumidores. Esta obligación de informar a los socios debe reforzarse en el área económica.

En el sector bancario se adoptó la Ley número 289/2004 que contempla el régimen judicial de los contratos de crédito para necesidades personales, diseñada para individuos. Esta ley establece las condiciones para cerrar un contrato de crédito para necesidades personales y contiene algunas cláusulas para proteger a los consumidores.

Otra norma diseñada para proteger al consumidor en el área económica es la OG 85/2004 que contempla la protección del consumidor cuando cierra y ejecuta contratos a distancia. Estas estipulaciones legales aluden a las condiciones de informar a los consumidores en los contratos económicos contemplando los servicios bancarios, tarjetas de crédito, seguros, pensiones privadas y las inversiones financieras.

Estas normas legales junto con las de la ley común, defienden los intereses de los consumidores en el área financiera y aseguran suficiente protección a la parte "débil" de los contratos económicos.

EL DERECHO A LA INFORMACIÓN

El derecho a la información: el proveedor de servicios tiene la obligación de informar al consumidor a tiempo, correctamente y por completo sobre los elementos esenciales del contrato. El proveedor tiene la obligación de probar que ha cumplido con esta tarea.

El derecho a la denuncia unilateral del contrato, con mención de las condiciones del consumidor de las que se hace uso.

INCUMPLIMIENTOS EN LA OBLIGACIÓN DE INFORMAR Y SU PENALIZACIÓN

Tras analizar algunos contratos, el resultado fue que no todas las unidades bancarias explicaban claramente ciertos términos como la hipoteca, la concesión, etc., de forma que los consumidores lo entendieran.

No existe una especificación clara sobre los porcentajes de penalización por un retraso en el pago de una cuota, su participación o la posibilidad del consumidor de cerrar unilateralmente un contrato con 30 días de aviso. Se pudo comprobar que los contratos carecían de una elaboración clara y comprensible y que faltaba información con respecto al período de finalización, modos de ejecución, suspensión o paro del servicio. Así mismo los términos, notificaciones, condiciones del depósito y condiciones aseguradoras eran confusas para el consumidor.



Italia

El fraude en los medios de pago en la legislación italiana

Al margen del fraude tradicional en los métodos de pago como el realizado con billetes o cheques falsos, los fraudes relacionados con las tecnologías de la información considerados en Italia también como "delitos informáticos", son cada vez más comunes.

1. MARCO LEGISLATIVO GENERAL

LA PROTECCIÓN AL CONSUMIDOR EN LA CONSTITUCIÓN

La Constitución Italiana data de 1948, periodo en el que la emisión de una protección del consumidor era prácticamente desconocida en Europa. Por razones políticas circunstanciales, la Constitución Italiana está centrada en la protección de la mano de obra, más que en el aumento del bienestar del consumidor. Se puede encontrar una pequeña muestra de la protección del consumidor en la sección 47, en la medida en que se establece que “La República anima y protege los ahorros del tipo que fueren”.

REGULACIÓN DE LOS MÉTODOS DE PAGO DEL CÓDIGO CIVIL (TEORÍA DE UN CONTRATO)

El Código Civil italiano data de 1942, periodo en el que la emisión de protección del consumidor era prácticamente desconocida en Europa. Por lo tanto, en el Código Civil, los métodos de pago se regulan independientemente de la calidad subjetiva del consumidor o profesional. La obligación de pagar una cantidad de dinero tiene carácter objetivo y no es posible librarse de la responsabilidad de pagar, a no ser que den pruebas de que la infracción de tal obligación de pagar se debe a algo material y a la imposibilidad general de cumplir con la obligación que no se debe a sí mismo (TRIMARCHI P., *Instituzioni di diritto privato* (Instituciones de derecho privado), XVI ed. Milán, 2005, 300). Al amparo de la sección 1277 del Código Civil, “las deudas monetarias se abonan en efectivo con curso legal en el estado, en el momento de pago y por su valor nominal”. Sin embargo, este principio general debe estar coordinado por leyes para la protección de blanqueo de capitales, que prohíbe el pago en efectivo por encima de una cantidad determinada. En términos generales, y más allá de las enmiendas (la última se ha introducido en la sección 1, párrafo 1, de la Ley nº 133 del 6 de agosto de 2008), en Italia, está prohibido utilizar efectivo para pagos superiores a 12.500,00 € incluso aunque existan límites inferiores para determinados pagos (por ejemplo, se permiten pagos en efectivo a abogados, médicos, etc. hasta 500,00 € hasta el 30 de junio de 2009 y hasta 100,00 € a partir de esa fecha).

2. OTRA LEGISLACIÓN SOBRE LA MATERIA

LOS FRAUDES CON TARJETA DE CRÉDITO

El uso indebido de las tarjetas de crédito está regulado en Italia desde 1991: la sección 12 de la Ley nº 197 del 5 de julio de 1991 establece que:

“Cualquiera que, con animo de lucro para él o para una tercera parte, utilice de manera ilegal, sin ser el tenedor legítimo, tarjetas de crédito o realice pagos con las mismas, o cualquier otro documento similar que le permita obtener efectivo o adquirir bienes o servicios, será castigado con penas de cárcel de uno a cinco años y con multas de 600.000 a 3 millones de liras.

Del mismo modo, se castigará a cualquiera que, con ánimo de lucro para sí mismo o para un tercero, falsifique o modifique tarjetas de crédito, pagos o cualquier otro documento similar que le permita obtener efectivo o adquirir bienes o servicios o tener, transferir, adquirir las mencionadas tarjetas o documentos de origen ilegal o cualquier tipo de falsificación, modificación u órdenes de pago derivadas de las mismas.

Esta provisión está contenida ahora, exactamente en los mismos términos que antes, en la sección 55, párrafo 9 de la Ley (D.Lgs.) nº 231 del 21 de noviembre de 2007 (que ha revocado a la sección 12 de la ley nº 197 anterior), segura por el hecho de que la cantidad de la multa está ahora expresada en euros y va de 310,00 a 1.550,00.

Las implicaciones criminales de fraude por uso indebido de tarjetas de crédito parecen estar lo suficientemente cubiertas por este tipo de delito, sin embargo, en la práctica, pueden surgir problemas graves por el hecho que el autor de los fraudes puede mantenerse en el anonimato, residir en una jurisdicción remota o incluso, aunque esté en el territorio nacional italiano, puede declararse insolvente a la hora de compensar a la víctima.

La práctica habitual de emisión de las tarjetas de crédito es la de reembolsar a la víctima del uso indebido (uso de tarjetas robadas con la firma falsificada o uso de información de tarjetas de crédito robadas y utilizadas a través de Internet sin la suscripción del tenedor de la tarjeta).

Probablemente ésta sea la razón de que la investigación de la jurisprudencia no muestre ningún litigio civil signifi-

cativo en la materia, como puede ser una de las víctimas solicitando una compensación al emisor de la tarjeta de crédito en lugar de hacerlo al autor del delito.

La jurisprudencia se centra más en las relaciones entre el emisor de la tarjeta de crédito y el comerciante, estableciendo una lista de obligaciones para cada uno y poniendo en riesgo de uso indebido a uno o al otro de acuerdo con determinadas circunstancias (por ejemplo Cassazione civile, sez. III, 14 de julio de 2006, no. 16102 (Casación civil, sez III), Soc. Trattoria Quattro Venti Vs. Servizi Interbancari).

Sin embargo, un estudio sobre las relaciones entre los emisores de la tarjeta de crédito y los comerciantes radica fuera del alcance de este cuestionario y la conferencia que tendrá lugar en Italia tendrá que centrarse más bien en la investigación de los posibles daños a los tenedores de tarjetas de crédito.

De hecho, dado el aumento del uso de Internet, podría ocurrir que los emisores de la tarjeta de crédito cambien las prácticas anteriormente mencionadas imponiendo a las víctimas del uso indebido más y más límites. En lo referente a este problema, por favor, diríjase a la referencia posterior en la sección “Pagos en línea”.

LAS TRANSFERENCIAS

No existen estatutos concretos o jurisprudencia relativos a las transferencias.

EL FRAUDE COMETIDO A TRAVÉS DEL CHEQUE

Las leyes de cheques datan de 1931 (con el Decreto Real nº 1736 del 21 de diciembre de 1933) como dispositivo de mejora de la Convención Internacional de Ginebra del 19 de marzo de 1931. Por lo tanto, la mayor parte de esta área está relacionada con la unificación de la ley, aplicable a todos los estados miembros ratificados.

No existen estatutos concretos o jurisprudencia en cheques, con regencia a consumidores.

LOS PAGOS ON LINE

Supone que el pago, estrictamente conectado a la tecnología de la información, podría dar origen a los llamados “delitos informáticos”. Para cifras y estadísticas, por favor, diríjase a la posterior sección D).

EL CRIMEN CIBERNÉTICO EL SISTEMA LEGAL ITALIANO

Como se explica en la sección anterior, el uso indebido de las tarjetas de crédito, está regulado en Italia desde 1991.

Al amparo de la legislación de la UE, desde 1993, la ley 547/93, Italia introdujo una serie de provisiones al derecho criminal dirigidos al castigo de los crímenes informáticos.

Los crímenes instituidos recientemente son los que siguen:

Fraude informático: similar al fraude tradicional, con la diferencia de que éste se ejecuta a través de dispositivos informáticos. Por lo tanto, la Ley 547 de 1993 añade al Código Penal, la sección 640-ter para penar a cualquiera que busque un beneficio ilegal a través de la interferencia del procesamiento de datos electrónicos;

Falsificación de documentos informáticos: para este propósito, los documentos informáticos están considerados del mismo modo que los tradicionales, y la sección 491-bis del Código Penal, extiende a los mismos los castigos previstos para los documentos públicos y privados.

Ataque a la integridad de la información: la recién introducida sección 635-bis del Código Penal castiga el daño de ordenadores y redes de telecomunicación, la sección 615 quinquies la propagación de virus y malware, la sección 392 de daños a la propiedad, ahora castiga también los llamados bienes informáticos;

Ataque a la privacidad de datos y de la comunicación informática: las cifras introducidas últimamente, son el acceso abusivo a redes informáticas o de telecomunicaciones (sección 615-ter del Código Civil), posesión ilegal y propagación de códigos de acceso (sección 615-quater del Código Penal), publicación de contenidos de documentos confidenciales (sección 621 del Código Penal) e incluyen los documentos informáticos. También la interceptación, la modificación informática y la correspondencia de telecomunicaciones están ahora penadas por la sección 617-quater del Código Penal, como lo está la instalación de dispositivos con intención de interceptar o dificultar tal correspondencia (sec-

ción 617-quinquies del Código Penal).

Por último, no debemos olvidarnos de que ya había cifras anteriores al delito, como la proporcionada al amparo de la sección 494 del Código Civil (sustitución de una persona) que, sin ninguna enmienda, podría ajustarse perfectamente a los crímenes cibernéticos, como la suplantación de la identidad,

Por lo tanto, las implicaciones criminales de fraude en métodos de pago en línea parecen estar suficientemente cubiertas por los diferentes tipos de crimen, convencional o de nueva institución, enumerados en el Código Civil italiano.

Sin embargo, en la práctica, pueden surgir problemas graves por el hecho de que el autor de los fraudes puede mantenerse en el anonimato, residir en una jurisdicción remota o incluso, aunque esté en el territorio italiano, puede declararse insolvente para compensar a la víctima.

Una primera investigación no muestra ningún litigio civil significativo en la materia, como la de las víctimas que reclaman compensación por emisión de tarjetas, banca electrónica, etc. en lugar del autor del delito.

Las leyes de protección de datos (en Italia, la revisión más reciente del código de protección de datos, data de 2003) parecen no tener ningún efecto, o muy poco desde la perspectiva de la protección del consumidor, mientras el lazo burocrático de la actividad comercial se incrementa.

En otras palabras, las secciones 34 del Código de protección de datos de 2003, especifican requisitos concretos en caso de procesamiento de datos electrónicos, pero no cubren el caso en el que la banca electrónica o el emisor de una tarjeta de crédito alegan que la infracción de la protección de datos se debe a que el consumidor no mantuvo a salvo la información relevante y los códigos secretos.

¿CÓMO PUEDE EL CONSUMIDOR PROBAR QUE LA BANCA ELECTRÓNICA PUBLICÓ LOS CÓDIGOS SECRETOS Y NO ÉL MISMO?

Algunos académicos sugieren extender el principio de fiabilidad del producto también a servicios como tarjetas de crédito y banca electrónica, como se especifica al amparo de la Directiva de la CE 85/374 (por la que los productores y vendedores se consideran igualmente responsables de los daños causados por los productos que han producido/venido, a no ser que se pruebe que los daños se deben a circunstancias imprevisibles).

Esto también podría responder al análisis económico de los criterios de la ley, según la que los daños deben recaer, en parte o en su totalidad, en el actor económico que tiene la parte de beneficios más grande en esa actividad concreta (por ejemplo, el emisor de la tarjeta o el banquero electrónico).

De este modo, la responsabilidad cambiaría, en parte o en su totalidad, de la víctima del crimen cibernético a las compañías que operan en el sector.

Aunque podríamos apreciar y estamos de acuerdo en esa sugerencia, las leyes civiles aplicables existentes ofrecen muy pocas pistas para la investigación de una solución previsible.

EL PAGO A TRAVÉS DEL TELÉFONO MÓVIL

No existen estatutos concretos o jurisprudencia en pagos con el teléfono móvil, que hagan referencia a los consumidores.

En este momento, Italia está trabajando en la mejora, a nivel nacional, de la Directiva de servicios de pago 2007/64/EC para noviembre de 2009. Esta directiva considera también los servicios de pago con dispositivos digitales, como los teléfonos móviles o los ordenadores.

3. LAS PECULIARIDADES EN LA LEY APLICABLE

¿CÓMO SE ENFRENTA A ESTE TIPO DE CRIMEN CIBERNÉTICO EL SISTEMA LEGAL ITALIANO?

El uso indebido de las tarjetas de crédito está regulado en Italia desde 1991: la sección 12 de la Ley nº 197 del 5 de julio de 1991 establece que:

“Cualquiera que, con ánimo de lucro para él o para una tercera parte, utilice de manera ilegal, sin ser el tenedor legítimo, tarjetas de crédito o realice pagos con las mismas, o cualquier otro documento similar que le permita obtener efectivo o adquirir bienes o servicios, será castigado con penas de cárcel de uno a cinco años y con multas de 600.000 a 3 millones de liras. Del mismo modo, se castigará a cualquiera que, con ánimo de lucro para sí mismo o para un tercero, falsifique o modifique tarjetas de crédito, pagos o cualquier otro documento similar que le permita obtener efectivo o adquirir bienes o servicios o tener, transferir, adquirir las mencionadas tarjetas o documentos de origen ilegal o cualquier tipo de falsificación, modificación u órdenes de pago derivadas de las mismas.

Al amparo de la legislación de la UE, desde 1993, con la ley 547/93, Italia introdujo una serie de provisiones al derecho criminal dirigidos al castigo de los crímenes informáticos.

A saber, los crímenes instituidos recientemente son los que siguen:

Fraude informático: similar al fraude tradicional, con la diferencia de que éste se ejecuta a través de dispositivos informáticos. Por lo tanto, la Ley 547 de 1993 añade al Código Penal, la sección 640-ter para penar a cualquiera que busque un beneficio ilegal a través de la interferencia del procesamiento de datos electrónicos;

Falsificación de documentos informáticos: para este propósito, los documentos informáticos están considerados del mismo modo que los tradicionales, y la sección 491-bis del Código Penal, extiende a los mismos los castigos previstos para los documentos públicos y privados.

Ataque a la integridad de la información: la recién introducida sección 635-bis del Código Penal castiga el daño de ordenadores y redes de telecomunicación, la sección 615 quinquies la propagación de virus y malware, la sección 392 de daños a la propiedad, ahora castiga también los llamados bienes informáticos;

Ataque a la privacidad de datos y de la comunicación informática: las cifras introducidas últimamente, son el acceso abusivo a redes informáticas o de telecomunicaciones (sección 615-ter del Código Civil), posesión ilegal y propagación de códigos de acceso (sección 615-quater del Código Penal), publicación de contenidos de documentos confidenciales (sección 621 del Código Penal) e incluyen los documentos informáticos. También la interceptación, la modificación informática y la correspondencia de telecomunicaciones están ahora penadas por la sección 617-quater del Código Penal, como lo está la instalación de dispositivos con intención de interceptar o dificultar tal correspondencia (sección 617-quinquies del Código Penal).

Por último, no debemos olvidarnos de que ya había cifras anteriores al delito, como la proporcionada al amparo de la sección 494 del Código Civil (sustitución de una persona) que, sin ninguna enmienda, podría ajustarse perfectamente a los crímenes cibernéticos, como la suplantación de la identidad,

Por lo tanto, las implicaciones criminales de fraude en los métodos de pago parecen estar suficientemente cubiertas por los diferentes tipos de crimen, convencional o de nueva institución, enumerados en el Código Civil italiano.

Sin embargo, en la práctica, pueden surgir problemas graves por el hecho de que el autor de los fraudes puede mantenerse en el anonimato, residir en una jurisdicción remota o incluso, aunque esté en el territorio italiano, puede declararse insolvente para compensar a la víctima.

Una primera investigación no muestra ningún litigio civil significativo en la materia, como la de las víctimas que reclaman compensación por emisión de tarjetas, banca electrónica, etc. en lugar del autor del delito.

La conferencia que tendrá lugar en Italia tiene que tener como objetivo buscar la investigación en este aspecto principal y proporcionar una posible guía para la decisión en casos futuros.

Las leyes de protección de datos (en Italia, la revisión más reciente del código de protección de datos, data de 2003) parecen no tener ningún efecto, o muy poco desde la perspectiva de la protección del consumidor, mientras el lazo burocrático de la actividad comercial se incrementa.

En otras palabras, las secciones 34 del Código de protección de datos de 2003, especifican requisitos concretos en caso de procesamiento de datos electrónicos, pero no cubren el caso en el que la banca electrónica o el emisor de una tarjeta de crédito alegan que la infracción de la protección de datos se debe a que el consumidor no mantuvo a salvo la información relevante y los códigos secretos.

¿Cómo puede el consumidor probar que la banca electrónica publicó los códigos secretos y no él mismo?

Algunos académicos sugieren extender el principio de fiabilidad del producto también a servicios como tarjetas de crédito y banca electrónica, como se especifica al amparo de la Directiva de la CE 85/374 (por la que los productores y vendedores se consideran igualmente responsables de los daños causados por los productos que han producido/vendido, a no ser que se pruebe que los daños se deben a circunstancias imprevisibles).

Esto también podría responder al análisis económico de los criterios de la ley, según el que deben recaer los daños, en parte o en su totalidad, en el actor económico que tiene la mayor parte de beneficios en esa actividad concreta (por

ejemplo, el emisor de la tarjeta o la banca electrónica).

De este modo, la responsabilidad cambiaría, en parte o en su totalidad, de la víctima del crimen cibernético a las compañías que operan en el sector.

Aunque podríamos apreciar y estamos de acuerdo en esa sugerencia, las leyes civiles aplicables existentes ofrecen muy pocas pistas para la investigación de una solución previsible.

4. EL FRAUDE EN CIFRAS

CLASIFICACIÓN DE FRAUDES REALIZADA POR LA COMISIÓN EUROPEA

Las categorías establecidas al amparo del informe sobre fraude de la Comisión CE en lo que respecta a los métodos de pago no en metálico en la UE el 22 de abril de 2008, son las siguientes:

Uso indebido de tarjetas de crédito perdidas o robadas y falsificación y posterior uso de tarjetas falsificadas.

El fraude superficial, por ejemplo, la copia ilegal de la banda magnética de la tarjeta;

fraude cuando la tarjeta no está presente, por ejemplo el uso indebido de información de la tarjeta obtenida de manera ilegal en pedidos por correo o telefónicos, pero sobretudo en pagos a través de Internet;

Fraudes de banca electrónica, por ejemplo el fraude de adquisición de la cuenta corriente a través del uso indebido de la información bancaria del cliente, obtenida a través de varias técnicas, incluidas la falsificación, el phishing, el pharming, los troyanos (u otros virus o malware parecido), el pirateo de bases de datos, los fraudes de personal, etc.

Tanto el fraude de la tarjeta ausente como el de la banca electrónica son, de facto, variantes de un fenómeno de fraude o robo mayor que, debido al creciente uso de las redes de comunicación electrónica, se está convirtiendo en una categoría del problema de delitos cibernéticos, que abarca más supuestos.

LAS ESTADÍSTICAS RECIENTES RECOGEN EL AUMENTO DEL RIESGO DE ROBO DE INFORMACIÓN PERSONAL

De acuerdo con las estadísticas¹ recientes, Italia registra un aumento significativo del riesgo de robo de información personal e identidad.

Las víctimas potenciales más probables en este tipo de delito cibernético son hombres entre los 30 y los 49 años, porque, potencialmente, tienen un más opciones de obtener crédito y porque, más que otros, hacen y dejan las llamadas “huellas personales” por sus hábitos de vida (viajes, reservas de hoteles, cenas fuera, compra de bienes, solicitud de préstamos, etc.).

Desde el punto de vista del trabajador, los profesionales son las víctimas potenciales más visibles. Por ejemplo, para profesionales que necesitan estar registrados en determinados registros públicos, los datos personales son, normalmente, de dominio público, a los que puede acceder cualquiera a través de Internet.

Los profesionales que están entre los treinta y los cuarenta años, prestan más atención a determinadas precauciones mínimas: de acuerdo con las estadísticas anteriormente mencionadas, menos del 35% de hombres en este rango de población destruye los documentos antes de tirarlos a la papelera y sólo una media del 37%, controla el estado de sus cuentas. En general, la gente a la que se ha entrevistado, se limita a declarar que mantiene la información en un “lugar seguro”.

Otro rango de alto riesgo, es la población representada por los jóvenes entre 20 y 29 años, que normalmente no tienen cuidado y se quedan en la superficie a la hora de proteger y desvelar sus datos personales: el 32% de la gente entrevistada declaró no haber pensado nunca, o raramente, en la protección de sus datos personales. Es más, los jóvenes tienen un conocimiento muy limitado del mencionado fenómeno criminal: aunque más de un 90% es consciente de los fraudes en las tarjetas de crédito y alrededor de un 70% ha oído hablar de la “suplantación de identidad”, el 72% de los jóvenes en ese rango de edad no sabe, a pesar del uso masivo de Internet, lo que significa el término “phishing” y un 87% nunca ha oído hablar de la técnica de trashing o “revisión de la basura”.

Las técnicas de fraude actuales explotan más y más las posibilidades garantizadas por las nuevas tecnologías y se convierten, cada vez más, en técnicas sofisticadas y peligrosas, permitiendo al autor del fraude, en la mayor parte de los casos, mantenerse oculto. Además, esta actividad, evoluciona de una banda criminal a una estructura de bandas de criminales organizada.

Ser víctima de un robo de identidad, puede implicar consecuencias serias y desagradables, como la difamación, la confrontación con falsos testimonios como los indicios de uno mismo como deudor, o persona insolvente, estar sujeto a investigaciones policiales o a solicitudes de pago, con pocas o ninguna posibilidad de ser reembolsado.

De acuerdo con otras estadísticas², las cifras para identificar el robo crecen continuamente: sólo en 2006, se calcularon más de 17.000 intentos de robo (con un aumento del 55% si lo comparamos con 2005) para una cantidad total de dinero robado de más de 80 millones de euros (habiendo sido 46,5 millones de euros en 2005).

Durante junio de 2006 y julio de 2007, se informó a la policía de 1.400 casos de suplantación de identidad. En el 93% de los casos, las víctimas no fueron capaces de indicar el autor del crimen, que era anónimo.

El fraude, de media, ascendía a 5.301 euros.

LAS OPERACIONES QUE HAN DADO LUGAR A LA MAYOR PARTE DE LOS FRAUDES

La concesión de un préstamo para la compra de bienes (51,06%);

Solicitud de un préstamo (39,06%);

Los pagos con tarjeta de crédito han mostrado menos incidentes.

Finalmente, el hecho de que la víctima tarde demasiado en darse cuenta del fraude, es un dato muy preocupante: de media, suma unos 206 días, 580 en caso de emisión de tarjeta de crédito y 103 en caso de préstamos para la adquisición de bienes, con emisión simultánea de tarjeta de crédito.

El autor del crimen ha sido descubierto sólo en un 6% de los casos y normalmente, suele tratarse de comerciantes, familiares, amigos o colegas de la víctima.



República Checa

El fraude en medios de pago en la legislación checa

La armonización del marco legal checo fue completada el 1 de mayo del 2004, momento en el que la República Checa se adhirió a la Unión Europea.

1. MARCO LEGISLATIVO GENERAL

En general, podemos encontrar este tipo de regulación tanto en la Constitución como en Código Civil, que contempla tanto una teoría del contrato como la regulación de los medios de pago.

Otras compilaciones de interés son las que a continuación se enumeran:

Compilación del Código Penal número 140/1961.

Compilación del Código Civil número 40/1964.

Compilación del Código Comercial número 13/1991.

Compilación del Decreto número 254/2004, sobre la restricción de los pagos en efectivo.

Compilación del Decreto número 253/2008, sobre las medidas contra la legalización de beneficios provenientes de actividades delictivas y contra la fundación de terrorismo.

Compilación del Decreto número 253/2002, sobre transferencias de recursos financieros, recursos financieros económicos y sistemas de pago (ley sobre los sistemas de pago).

Decreto del Banco Nacional Checo, sobre la manera de realización de pagos entre bancos, contabilidad de las cuentas bancarias y los procedimientos técnicos de los bancos para la contabilidad correctiva.

2. OTRA LEGISLACIÓN SOBRE LA MATERIA

NORMATIVA EN MATERIA DE FRAUDES EN MEDIOS DE PAGO

Podemos enumerar algunas de las disposiciones legales sobre fraudes en medios de pago que no se efectúan en efectivo, incluyendo decretos relevantes de la UE transpuestos a la normativa checa.

97/489/EC: Recomendación de la Comisión, transacciones por pago electrónico.

87/598/EEC: Recomendación de la Comisión, Código Europeo de Conducta sobre los medios de pago.

97/7/EC: Directiva del Parlamento Europeo y la Comisión sobre la protección de los consumidores y contratos a distancia.

2001/413/EC y 2000/31/EC: Resoluciones del marco del Consejo para combatir el fraude y la falsificación de medios de pago que no se efectúan en efectivo.

2007/64/EC: Directiva del Parlamento Europeo y la Comisión sobre los servicios de pago.

Compilación de Decretos número 124/2002 de transposiciones de decretos de la Comisión Europea.



República Eslovaca

El fraude en medios de pago en la legislación eslovaca

La regulación eslovaca tiene presente los derechos y obligaciones del consumidor en el uso de algunos medios de pago, como las tarjetas, sin embargo aún le queda un largo camino por recorrer en muchos otros medios de pago.

1. MARCO LEGISLATIVO GENERAL

La Constitución Eslovaca contiene algunos artículos que, aunque no directamente (no se refiere en ningún momento a la categoría “consumidor”, si afectan a los derechos y protección de los consumidores. Entre ellos, podemos destacar:

- artículo 26, párrafo 1, 4 y 5 – derecho a la información
- artículo 36, párrafo c y art 40 – derecho a la protección de la salud
- artículo 46 – derecho a un Tribunal de justicia independiente.

Por su parte, el Código Civil eslovaco está basado en el anterior Código Civil Checoslovaco 40/1964 y contiene numerosas novedades y cambios que se han ido adoptando durante los últimos 44 años.

Normativa civil aplicable a los contratos en general:

- Decreto 40/1964 más sus novedades
- Contratos en general – párrafo 43 - 51
- Contratos del consumidor – 52 - 60
- Contrato de compra – párrafo 588 - 627
- Contrato de préstamo – párrafo 657 – 662
- Contrato de comisión – párrafo 774 – 777

- Contrato de seguro – párrafo 788 – 828

Por su parte entre la normativa específica de Consumo, podemos destacar:

- Decreto del consumidor 250/2007 efectivo desde el 1 de julio del 2007
- Derechos del consumidor – párrafo 3
- Obligaciones de información – párrafo 11 – 18

En cuanto a los pagos en efectivo, se han llevado a cabo medidas desde los 90 para luchar a través de la legislación de impuestos contra el blanqueamiento de dinero poniendo límite en los pagos con dinero en efectivo fuera del sistema bancario, medidas que no han sido del todo eficaces.

2. OTRA LEGISLACIÓN SOBRE LA MATERIA

EL FRAUDE A TRAVÉS DE TARJETA DE CRÉDITO

El mal uso de las tarjetas de crédito se regula mediante el decreto de Sistemas de Pago número 510/2002, efectivo a partir del 31 de agosto del 2002. Este decreto contempla las obligaciones y la posibilidad de reclamar que tiene el consumidor contra el banco o el emisor de las tarjetas en caso de mal uso de las mismas.

Por su parte, el código penal número 300/2005 en su artículo 219, regula la falsificación y uso no autorizado de la tarjeta como medio de pago – la pena básica es de 1 a 5 años de prisión y de 5 a 12 años en casos especiales – categorizándolo de gran daño, asimismo regula las penas que conlleva ser miembro de un grupo organizado peligroso.

Aunque se puede considerar que las leyes son tan claras y suficientes en la práctica, existen muchos problemas en caso de que una tarjeta o la información de identificación de esta sea mal usada y como consecuencia el consumidor se viese perjudicado por una retirada ilegal de dinero de su cuenta bancaria. En la mayoría de los casos los bancos o emisores de tarjetas no están dispuestos a aceptar el punto de vista del consumidor o sus argumentos y normalmente declaran que el consumidor causó el problema y que el emisor de la tarjeta no cometió ningún fallo, sobre todo en casos donde se desconoce al autor del fraude, lo que es muy común.

LAS TRANSFERENCIAS

El decreto de Sistemas de pago número 510/2002, efectivo desde el 31 de agosto del 2002, regula en sus artículos 3 a 11 las transferencias nacionales y en los artículos 12 a 20 las internacionales. No hay ninguna regulación específica acerca de los consumidores.

LOS CHEQUES

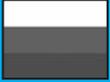
No hay ninguna regulación específica acerca de los consumidores.

PAGOS ON LINE

Los pagos on line están unidos a las tecnologías de la información – sistemas informática e internet. El Decreto de Sistemas de pago número 510/2002, efectivo desde el 31 de agosto del 2002, artículo 21a 24.

PAGOS POR MÓVIL

Así como no se han identificado leyes especiales para estos sistemas de pago, la implantación de la Directiva de los Servicios de Pago 2007/64/EC durante el próximo período podría cambiar la regulación sobre este medio de pago.



Bulgaria

El fraude en medios de pago en la legislación búlgara

La protección del consumidor no aparece reflejada en la Constitución, el Código de las obligaciones es el cuerpo principal de la ley que regula los derechos del consumidor.

1. MARCO LEGISLATIVO GENERAL

LA REGULACIÓN CONSTITUCIONAL Y CIVIL

El artículo 19 de la Constitución versa sobre la economía libre de mercado, basada en la iniciativa libre, donde la ley garantiza unas condiciones igualitarias para la actividad económica a las entidades individuales y legales protegiendo los derechos de los consumidores, luchando contra la competencia desleal y contra las prácticas de monopolio.

Los medios de pago se regulan en varios decretos, tenemos que destacar el Decreto de Protección al Consumidor, Decreto de los Servicios Económicos a Distancia, Decreto del Comercio Electrónico, y Decreto de la Transferencias económicas y Medios de Pago Electrónicos.

2. OTRA LEGISLACIÓN SOBRE LA MATERIA

LAS TARJETAS COMO MEDIO DE PAGO

Podemos destacar las siguientes disposiciones legales:

Artículo 60 del Decreto de Protección al Consumidor, uso ilegal de una tarjeta bancaria en contratos a distancia.

Artículo 27- 40a del Decreto de las Transferencias económicas y Medios de Pago Electrónicos trata los derechos y obligaciones de los emisores y titulares de los medios de pago electrónicos.

Artículo 249 del Código Penal debe ser revisado. Afirmar que los fraudes de los medios de pago, que causan daños materiales considerables, son sentenciados de 2 a 8 años de prisión y se le impone una multa de hasta el doble de la suma del fraude.

"Daños materiales considerables" significa el salario mínimo mensual en Bulgaria multiplicado por 14, es decir unas 3080 levas (1540 euros). Por lo tanto, los fraudes por menos de 3080 levas no están cubiertos por el artículo 249. Así que los "daños materiales considerables" deben excluirse del decreto.

LAS TRANSFERENCIAS, CHEQUES Y PAGOS ON-LINE

Los artículos 27- 40 a del Decreto de las Transferencias económicas y Medios de Pago Electrónicos tratan los derechos y obligaciones de los emisores y titulares de los medios de pago electrónicos.



Eslovenia

El fraude en medios de pago en la legislación eslovena

La protección del consumidor no aparece reflejada en la constitución. El eje central de la legislación de protección al consumidor es una Ley específica en Protección al consumidor.

1. MARCO LEGISLATIVO GENERAL

LA REGULACIÓN DE LOS MEDIOS DE PAGO EN EL CÓDIGO CIVIL

El cuerpo principal de la ley en este campo no es el Código Civil, sino el Código de las obligaciones. Además, se encuentran más especificaciones en la Ley de protección al consumidor y en la Ley de los medios de pago.

Las leyes mencionadas se fundamentan básicamente en los casos de sustracción de tarjetas y phishing.

Debemos destacar en el Código de obligaciones las siguientes disposiciones:

Art. 5: Concepto de conciencia en el cumplimiento de las obligaciones contractuales

Art. 6: Principio de prudencia

Art. 86-88: Condiciones de la nulidad del contrato

Art. 121-122: Términos y condiciones generales y su nulidad

Asimismo en la Ley de protección del consumidor:

Art. 23-24: Prohibición de términos contractuales desleales

Art. 45: Diligencia de los mensajes publicitarios no deseados

2. OTRA LEGISLACIÓN SOBRE LA MATERIA

Ley de modos de pago:

Art 9.: Contenido obligatorio de los términos y condiciones generales

Art. 13: Contenido obligatorio de la orden de pago (identificación...)

Art. 24: Obligación de compensar las transacciones de pago, resolución de disputas

Ley de la banca:

Art. 230: Resolución de disputas entre bancos y consumidores

Código Penal:

Art 154: Abuso de los datos personales

Art 225: Entrada no autorizada en un sistema de información

Art. 242: Invasión a un sistema de información

Art 309: Producción y adquisición de herramientas pensadas para acciones penales

Ley de comunicación electrónica:

Art. 109: diligencia de los mensajes publicitarios no deseados

Ley de protección de datos

LA REGULACIÓN DE LOS CHEQUES

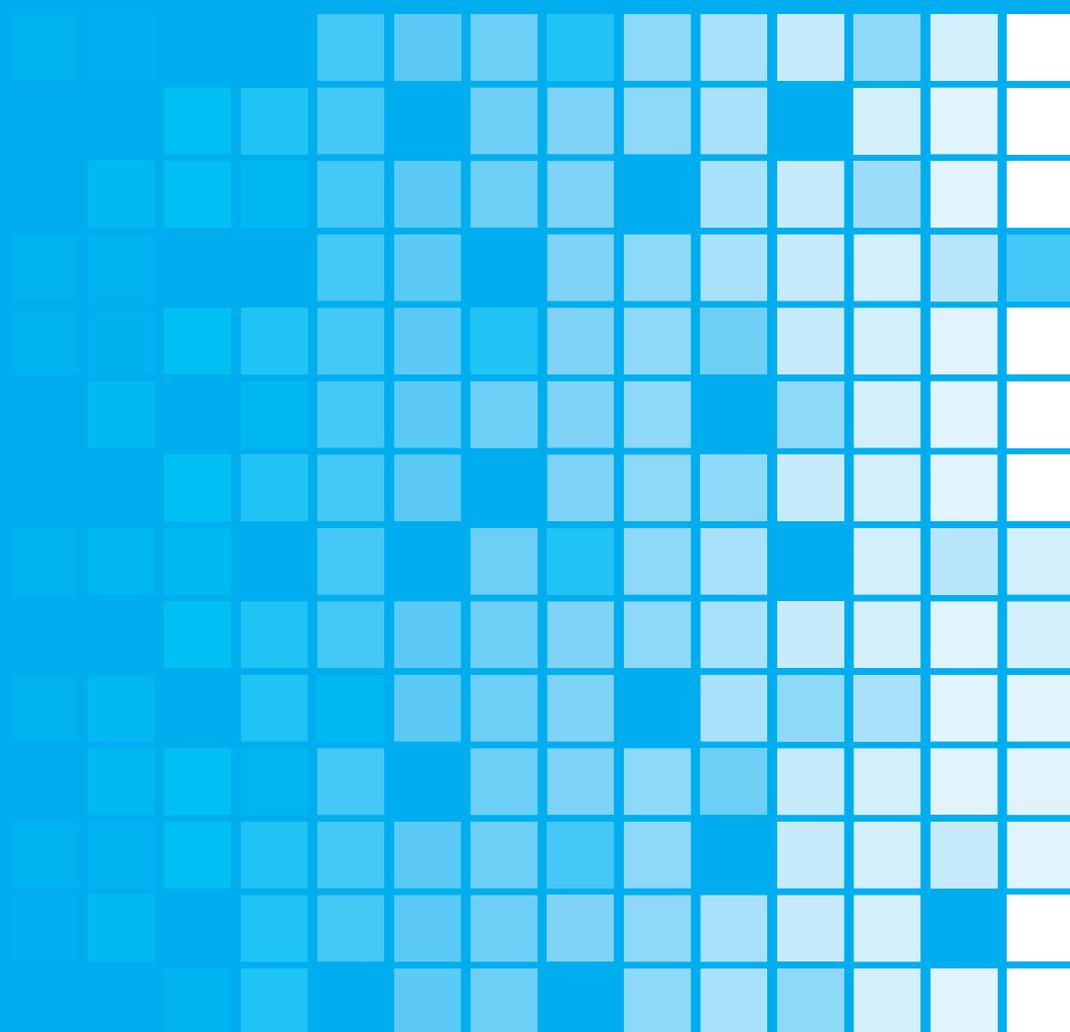
Los cheques están regulados por la Ley de cheques. Sin embargo, el uso de los cheques en Eslovenia hoy, es poco significativo. Ya no es un método de pago obligatorio. Algunos bancos ya no los ofrecen, los consumidores los obtienen en otras entidades tras hacer una solicitud especial. Esta es la razón por la que se propone omitir este campo en Eslovenia y concentrarse en otros más importantes.

LOS PAGOS A TRAVÉS DEL TELÉFONO MÓVIL:

La banca a través del teléfono móvil todavía no se ha desarrollado completamente en Eslovenia. Sólo una entidad bancaria ofrece este servicio, bastante complicado y utilizado en raras ocasiones por los consumidores.

Anexo III

Resolución extrajudicial de conflictos en Europa (países partners)



ANÁLISIS COMPARATIVO DE LOS “ADR” EN DISTINTOS PAÍSES DE EUROPA

Como última parte dentro de la toma de información de la situación de acceso a justicia, se solicitó a las asociaciones partners del proyecto, que remitieran informes sobre el estado del acceso a tribunales y a ADR (Resolución extrajudicial de conflictos) en su país.

Este estudio resulta tremendamente novedoso porque no se había manejado esta información de forma comparada hasta ahora. Con ello, se ha puesto de manifiesto la falta de información ya no sólo de los usuarios sino de las propias instituciones, con lo que de esta forma es difícil que surjan propuestas de mejora, se tomen ideas de otros países, etc.



Bulgaria

PROMOCIÓN DE LA ADR EN BULGARIA

- Los mecanismos para la resolución extrajudicial de conflictos en Bulgaria son relativamente recientes
- La posibilidad de recurrir a ellos cuando surgen problemas entre prestatario de bienes o servicios y consumidor es relativamente desconocida.

ASOCIACIÓN BÚLGARA PARA LA RESOLUCIÓN EXTRAJUDICIAL DE CONFLICTOS (2006)

- Desarrolla actividades de promoción y divulgación de la ADR
- Cooperación con instituciones y ONGs para facilitar el acceso a estos sistemas de resolución.
- Promover la mediación en general bajo las condiciones establecidas en la actual Ley de Mediación.

COMISIÓN DE CONCILIACIÓN EN CONFLICTOS POR PAGOS

Es un cuerpo independiente

Consta de:

- 2 representantes de la Asociación de Bancos Comerciales
- 2 representantes de la Comisión de Protección al Consumidor

Tiene potestad para actuar en:

- Conflictos sobre transparencia
- Conflictos sobre temas de pago electrónico



Italia

En Italia no existe legislación específica sobre vías extrajudiciales son los siguientes:

- mediación
- conciliación (el más utilizado)
- arbitraje
- ombudsman
- peritaje contractual

MEDIACIÓN

Poco utilizada en consumo. si ámbito familiar y administrativo dirigirse a centros de mediación o sociedades de mediación autorizadas la solicitud se envía a la secretaria de la cámara de arbitraje y mediación duración unos 30 días
coste máximo 80 euros entre los dos

CONCILIACION

Procedimiento extrajudicial para la solución amistosa de las controversias de naturaleza económica
inicio: en las cámaras de comercio, asociaciones de consumidores y centros de conciliación
conciliador experto imparcial e independiente
suele ser voluntario
rapidez, simplicidad, gastos reducidos y discreción

EL ARBITRAJE

- realizados por las cámaras de arbitraje y mediación
- 1 ó 3 árbitros imparciales e independientes de las partes
- clausula de compromiso previo
- arbitraje ritual: valor jurisdiccional. ejecutable
- arbitraje no ritual: valor contractual
- costes elevados

OMBUDSMAN

- controversias entre clientes y bancos
- primero acudir oficina de reclamaciones banco
- sus decisiones no vinculantes suelen ser cumplidas
- gratuito. controversias de menos de 5.165 euros

CLASS ACTIONS

- utilizadas frecuentemente también frente a la banca
- actualmente hay varios proyectos de ley sobre este tema
- solo el gobierno puede realizarlas. ¿¿inconstitucional?
- otra propuesta intenta extenderlo a otros grupos



Francia

1) SISTEMAS DE MEDIACION REGULADOS POR LEY

- a) energía
- b) acuerdos del banco
 - cada banco designa a uno o mas
 - para contratos firmados entre consumidor y el banco
 - decisión en un plazo de 2 meses
 - gratuito
 - un comité estudia y evalúa sus decisiones
 - datos: 19726 archivos 20% admisibles. 50% favorables total o parcialmente
- c) mediador de la república

2) SISTEMAS DE MEDIACION NO IMPUESTOS SINO CREADOS POR LAS EMPRESAS

- a) mediación del seguro
 - la federación francesa de empresas de seguros y los grupos de empresas mutuas de seguros los tienen
 - datos en 2005 recibió 1502 archivos
 - el 48% admisibles. de ese 48% el 47% se resolvió sin necesidad de decisión formalizada.
- b) mediador de la compañía de correos
- c) compañías del crédito (asociaciones de sociedades financieras)
 - incluye compañías de finanzas y establecimientos financieros de crédito.
 - 366 expedientes. mas del 50% decisiones favorables al consumidor
- d) mediador del snfc (compañía ferroviaria)
- e) comunicaciones electrónicas
- f) derechos de internet

PROBLEMAS según CLCV

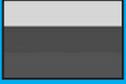
- falta de independencia
- no es vinculante
- plazos largos en ocasiones
- no interrumpe prescripción tribunales
- poca información entre consumidores

CUESTIONES POSITIVAS SEGÚN CLCV

- acceso libre
- uso de la equidad y no siempre la ley en sus decisiones

ACCIONES COLECTIVAS

- acción en interés colectivo para eliminar clausulas abusivas
- acción civil (varios perjudicados en actos no criminales)
- acción representativa: como la acción colectiva del art. 11 lec español. no se usa por su dificultad
- ejemplo concreto. clcv consigue sentencia frente a banco por mala información a clientes en sus inversiones.



Lituania

Los adr en lituania se enfocan como un establecimiento fuera de tribunales de los conflictos del consumidor (directiva de la comisión europea 98/257/ec) es una inspección de consumo realizada por el gobierno el consumidor primero debería presentar queja al empresario, no hay forma legal para ello. respuesta en unos 10 días. si no se llega a un acuerdo en el conflicto se hace una reclamación al gobierno, según la materia.

MATERIAS

- autoridad reguladora en comunicaciones
- comisión supervisora en los seguros
- energía
- 1)inspección de la energía estatal
- 2)comisión de control nacional para precios y energía
- 3)protección estatal del consumidor

CLASS ACTIONS

El código de procedimiento civil no habla de como las asociaciones representen a los consumidores. este papel es de la ley de protección al consumidor. estado, autoridades municipales pueden o deberían ser aceptadas como una parte en un procedimiento en defensa del interés público: para dar conclusión al caso.

CLASS ACTIONS II

Defendiendo el interés público la asociación de consumidores presenta una acción al tribunal. (gratuito)



Rumanía

ADR

Lo judicial es el método clásico
en los últimos años desarrollo de medios extrajudiciales

ARBITRAJE

Las partes proponen a los árbitros
resolución mas rápida de casos (1 año máximo)
costes mas bajos que los tribunales de justicia
expediente confidencial también
mediación opcional

DESVENTAJAS

Riesgo menor independencia
la ejecución solo ante tribunal
no acudir a tribunales después

MEDIACION

Año 2006

Se puede usar incluso después de un juicio
mediadores independientes asociados
no se excluye la mediación con entidades financieras, pero no se usa
muchos inconvenientes

CLASS ACTIONS

Relatividad de ejecuciones judiciales. sentencia solo afecta a quien la promueve sean uno o varios
Pero las decisiones sirven para asunto similares posteriores
Las asociaciones de consumidores pueden hacer procedimientos específicos.
pero la sentencia es para la asociación, no para consumidores



República Checa

DEMANDA EN CLASS ACTION

Parte del sistema de la ley desde 1.1.2003

-párrafo 85, sección 2 del código civil

-11-&159a, sección 2 del código civil

Hipotéticamente el primer demandante no conoce a los demás, si no existe tribunal para la situación del acuerdo entre el primer demandante y el demandado.

Ninguna posibilidad de reconocer una demanda de class action.

Ninguna obligación de dar al público información sobre los procedimientos.

ADR

Situación en república checa

Conflicto es generalmente resuelto por el tribunal

SOLUCIONES ALTERNATIVAS

- Arbitraje
- No apropiado para el consumidor
- Arbitro financiero
- Mediación
- Preparación de un nuevo sistema de adr



Bélgica

ADR:

- arbitraje
- defensores del pueblo
- mediación

MEDIACIÓN

- asuntos civiles, de consumo, pero también penales
- ley 21 febrero 2005
- normalmente voluntaria
- el resultado es otro nuevo contrato que regira a las partes
- participan abogados y peritos con frecuencia

ORGANIZACIONES DE MEDIACIÓN

- centro de arbitraje y mediación – cepina
- promover la mediación
- formada por profesores, abogados, etc
- no cualifica mediadores pero si designa el ideal centro de mediación mercantil de bruselas
- mercantil
- da una lista de mediadores para elegir

RESOLUCIÓN ELECTRÓNICA DE CONFLICTOS DE CONSUMO (ECODIR)

- mediación en línea
- beneficios por ser no presencial y darle a las empresas las quejas agrupadas
- el servicio es gratuito

CAMARA DE ARBITRAJE Y MEDIACIÓN

- asociación privada
- promueve el arbitraje y reúne mediadores en el ámbito del a cámara

ORGANISMO DE ARBITRAJE Y MEDIACIÓN (ABI)

OTROS: ORGANISMOS SECTORIALES DE MEDIACIÓN

- construcción
- familiar
- vehículos segunda mano
- mediación sector financiero
- dictamen no vinculante
- mediación seguros
- dictamen escrito en el plazo de 6 meses. tiene su propio estatuto

CLASS ACTIONS

- casos concretos de acciones colectivas:
- para prevenir racismo y xenofobia
- contra practicas que vulneren en el comercio la información y la protección al consumidor.
- actos contrarios a la ley de crédito al consumo
- medio ambiente



Polonia

ADR

Mediación por inspección comercial voluntaria
Oficinas regionales relevantes

ADR II

Corte permanente de arbitraje de consumo
16 cortes de consumo. dependen inspección comercial
gratuito pero informes se pagan
plazo resolución 1-2 meses

Arbitraje bancario
desde 2002.

coste 12 ó 5 euros.

40 días resolución

vincula al banco.

no al consumidor

requisitos:

-sólo el consumidor

-máximo 2000 euros

-primero dirigirse a la entidad

ADR IV

Corte arbitraje ombudsman seguros
Importe reclamado mayor de 250 euros.
Sentencia vinculante para las partes
Coste a partir de 30 euros

DATOS ADR 2006

Mediación : 2006 casos. 66'8% a favor consumidores

Arbitraje bancario: 807, sólo 15% a favor consumidores



Eslovaquia

MEDIACIÓN

Ley 420/2004

Aplicado a conflictos de familia, civil y mercantil una vez firmado el acuerdo es obligatorio para las partes características del acuerdo para que sea ejecutivo:

- forma notarial
- adoptado ante órgano de conciliación reconocido

ARBITRAJE

Ley 204/2002

Conflictos civiles y mercantiles
decisión ejecutable no necesario abogado
en un contrato se puede acordar la sumisión a arbitraje



Portugal

ADR

Centros de arbitraje. hay específicos para seguros y coche.
Justicia de paz (realiza la mediación voluntaria)
si no hay acuerdo se inicia procedimiento judicial

VENTAJAS

Rápidos
Gratuitos o costes bajos
Eficientes.
Plazo de resolución 2 meses

ACCIONES COLECTIVAS

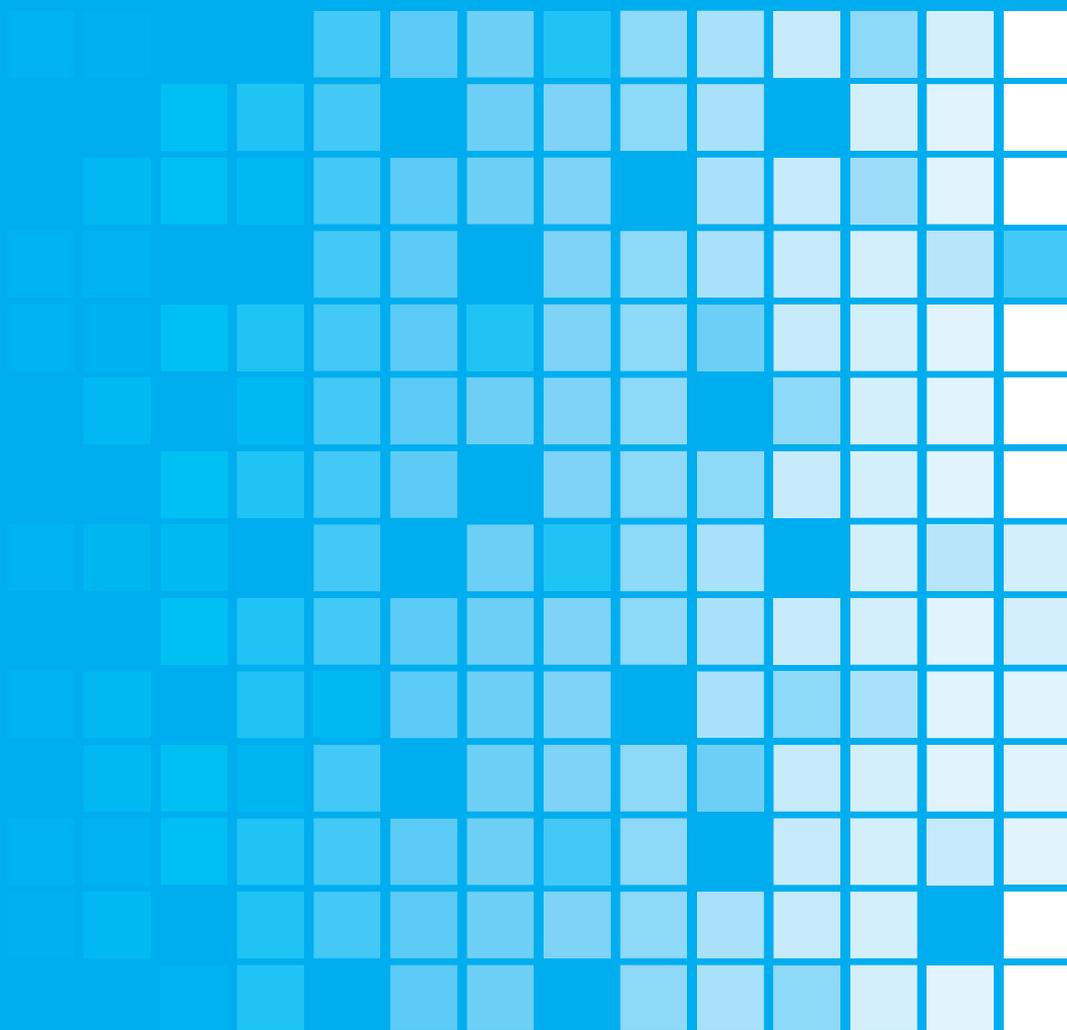
Legitimación. consumidor, gobierno, asociaciones de consumidores, asociaciones de profesionales, etc.
Poco usadas en Portugal. mas en el administrativo que el civil.

EXPERIENCIA APDC.

Contra compañía de telecomunicaciones. 11 años resolución.
Problemas, coste, plazo. propuesta reducir costes a estas acciones.

Anexo IV

Resumen de la normativa europea



DISPOSICIONES EMITIDAS POR LA UE SOBRE TRANSPARENCIA DE OPERACIONES Y PROTECCIÓN DE LA CLIENTELA

RECOMENDACIÓN 88/590/CEE, de la Comisión, de 17 noviembre, relativa a los sistemas de pago, y en particular a las relaciones entre titulares y emisores de tarjetas.

RECOMENDACIÓN 87/598/CEE DE LA COMISIÓN, de 8 de diciembre de 1987, sobre un código europeo de buena conducta en materia de pago electrónico (relaciones entre financieros, comerciantes organismos prestadores de servicios y consumidores).

RECOMENDACIÓN DE LAS COMUNIDADES EUROPEAS DE 17.11.1988, se establece la responsabilidad del emisor por la no ejecución o ejecución incorrecta de la órdenes de pago y por las operaciones no autorizadas por el titular. PERO, no basta con apreciar la falta de ejecución o la ejecución negligente, sino que además se exige que por parte del titular de la tarjeta no medie alguno de los supuestos de excepción: actuación fraudulenta del titular, negligencia grave, ni incumplimiento de la cláusula referente a la custodia de la tarjeta.

CÓDIGO DE BUENA CONDUCTA DE LA BANCA EUROPEA con respecto a los sistemas de pago mediante tarjeta, de 14 noviembre de 1990.

RECOMENDACIÓN 97/489/CE, DE LA COMISIÓN, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago. (Contiene la información mínima que deberá facilitarse al cliente en relación a las transacciones efectuadas mediante aquéllos). NO VINCULANTE, pero muy importante.

El emisor (E.F) se responsabiliza de la no ejecución o ejecución defectuosa de las transacciones del titular, de las transacciones no autorizadas por éste o de cualquier error atribuible al emisor en relación con la gestión de la cuenta del titular, asumiendo las consecuencias financieras derivadas de éstos.

LA DIRECTIVA 97/5/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de enero de 1997, relativa a las transferencias transfronterizas.

REGLAMENTO Nº 2560/2001, del Parlamento Europeo y del Consejo, de 19 diciembre de 2001, sobre los pagos transfronterizos en euros.

LA DECISIÓN MARCO DEL CONSEJO DE 28 MAYO DE 2001, relativa a la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo.

DIRECTIVA 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 noviembre de 2007, sobre servicios de pago en el mercado interior.

DIRECTIVA 2008/48/CE, del Parlamento Europeo y del Consejo, de 23 abril de 2008, relativa a los contratos de crédito al consumo.

ACTUACIONES CONTRA EL FRAUDE

Espacio de Libertad, seguridad y Justicia plasmado en el Tratado de Ámsterdam (en vigor desde 1999), hacia un auténtico Espacio Común icia Europeo, que implica la creación de: un Tribunal Penal Europeo y una Fiscalía Europea, y que proporciona a los Estados dos instrumentos:

1. la armonización de las legislaciones y
2. el principio de reconocimiento mutuo de resoluciones judiciales (instrumento de las Decisiones Marco).

Como último eslabón de la integración estaría el **Tratado para una Constitución para Europa, firmado en Roma el 29 de octubre de 2004** que se encuentra en proceso de ratificación.

La Decisión Marco del Consejo de 28 mayo de 2001, relativa a la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, cuyos objetivos son:

- a) procurar que todo fraude en el que se vea envuelto un medio de pago distinto del efectivo se convierta en infracción con sanciones efectivas en todos los EEMM y,
- b) que se creen mecanismos de cooperación entre Estados Miembros y entre servicios u organismos públicos o privados con el fin de perseguir eficazmente esas infracciones.

- CONDUCTAS QUE SE INCLUYEN:

- a) el hurto o apropiación indebida de un instrumento de pago.
- b) la alteración o falsificación de un instrumento de pago con la finalidad de su utilización fraudulenta.
- c) recepción, obtención o transporte, venta o cesión a otro o tenencia de instrumentos de pago obtenidos mediante apropiación indebida, alterado o falsificado.

Convención sobre Ciber - criminalidad del Consejo de Europa de 23.11.2001

- Su puesta en práctica representa el instrumento internacional de la lucha contra la delincuencia informática más destacado.

- Texto firmado por más de una treintena de países de todo el mundo todavía que a fecha de hoy sigue un lento proceso de ratificaciones.

- Se incluyen medidas que los Estados deben adoptar en sus legislaciones nacionales, tanto en lo relativo a Derecho penal como a Derecho procesal penal, CON EL FIN DE LOGRAR UNA ARMONIZACIÓN de las distintas legislaciones penales de los países signatarios.

- Para ello propone varias infracciones que deberán ser incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales, algunos de los cuales poseen especial incidencia en los supuestos relativos a los abusos con medios electrónicos de pago.

Un primer grupo de infracciones lo constituyen los **hechos contrarios a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos**. Dentro de este grupo se incluyen las conductas de acceso ilegal injustificado a todo o parte de un sistema informático.

El segundo grupo de conductas las denomina el Convenio Infracciones informáticas, y en ellas se incluye la **falsedad informática y el fraude informático**, con evidente repercusión para los supuestos de delitos cometidos con o sobre medios electrónicos de pago.

La Decisión Marco del Consejo de 28 de mayo de 2001, relativa a la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo

Definición medios de pago distintos del efectivo: todo instrumento material, exceptuada la moneda de curso legal que por su naturaleza específica permita, por sí sólo o junto con otro instrumento, al titular o usuario transferir dinero o un valor monetario y que esté protegido contra las imitaciones o la utilización fraudulenta. Esta descripción descarta no sólo el dinero en efectivo (billetes y monedas de curso legal) sino también el dinero electrónico en sentido estricto al carecer de soporte material.

El objetivo: procurar, por una parte, que todo fraude en el que se vea envuelto un medio de pago distinto del efectivo se convierta en infracción con sanciones efectivas en todos los EEMM y, por otra parte, que se creen mecanismos de cooperación entre Estados Miembros y entre servicios u organismos públicos o privados con el fin de perseguir eficazmente esas infracciones.

Así SE INCLUYEN:

- a) el hurto o apropiación indebida de un instrumento de pago.

- b) la alteración o falsificación de un instrumento de pago con la finalidad de su utilización fraudulenta.
- c) recepción, obtención o transporte, venta o cesión a otro o tenencia de instrumentos de pago obtenidos mediante apropiación indebida, alterado o falsificado.

Plan de acción de la UE (2004-2007) para la prevención del fraude de los medios de pago distintos del efectivo

Se fija por parte de la Comisión las prioridades para mantener y mejorar la cooperación entre todos los actores:

- Reconsiderar el sistema de transmisión de datos a nivel europeo
- Reorganizar el grupo de expertos en materia de prevención del fraude (GEPF) de cara a la ampliación de la Unión.
- Reforzar la seguridad de los sistemas de pago e implicar a los ciudadanos.
- Tener en cuenta las evoluciones técnicas

La Directiva 2007/64/CE del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior

Garantiza un nivel de protección elevado gracias a los requisitos en materia de información y a la definición de los derechos y obligaciones de los usuarios y de los proveedores de servicios de pago.

Regula:

- La ejecución de transferencias,
- Los pagos a través de tarjetas
- Las domiciliaciones
- La emisión o adquisición de instrumentos de pago o el envío de dinero.

Derechos para los consumidores

Transparencia de las condiciones y requisitos de información claros y concisos y GRATUITOS para todos los proveedores de servicios de pago.

Armonización básica de los derechos y obligaciones en relación con la prestación y utilización de los servicios de pago.

Responsabilidad del usuario de servicios de pago: en caso de utilización fraudulenta de un instrumento de pago la responsabilidad del usuario (excluidos los empresarios) estará limitada a 150 euros.

Condiciones de rectificación: según las cuales el usuario de servicios de pago tiene la posibilidad de rectificar una operación de pago no autorizada o ejecutada incorrectamente siempre que lo notifique a más tardar a los 13 meses de la fecha del adeudo, aunque existe posibilidad de convenir otro plazo entre las partes.

ÁMBITO PENAL

Artículo 248.1 : La estafa

Artículo 248.2 : La estafa electrónica

Artículo 386 : Falsificación de moneda (por asimilación)

Artículo 238: Robo con fuerza en las cosas

Artículos 197.1 y 2 : Revelación de secretos

Otros artículos: 263, 264.2, 255

ÁMBITO CIVIL

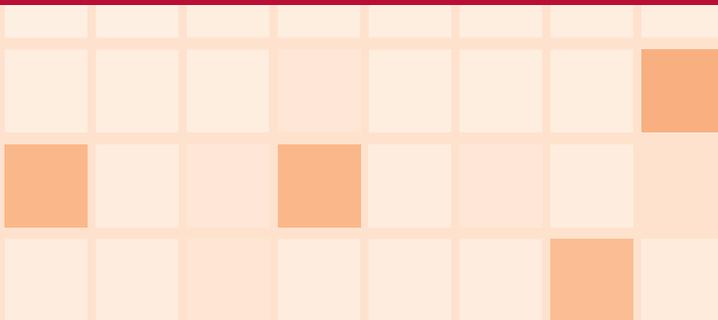
Código Civil: Regulación de la culpa y la negligencia. La Buena Fe

Ley Cambiaria y del Cheque

Reguladora de estos efectos distintos del efectivo. Culpa del consumidor

Ley Ordenación del Comercio Minorista

Cargos indebidos



SEDES DE ADICAE

Servicios Centrales ADICAE
C/ Gavín, 12 local 50001 **Zaragoza**
Tfno. 976 390060 - Fax 976 390199
aicar.adicae@adicae.net

Madrid
Embajadores, 135 1º C int. - 28045 **Madrid**
Tfno. 91 5400513 Fax 91 5390023

Catalunya
c/ Entença, 30 entlo. 1º - 08015 **Barcelona**
Tfno. 93 3425044 Fax 93 3425045

Comunidad Valenciana
Av. Pérez Galdós, 97 pta.1 - 46018 **Valencia**
Tfno. 96 3540101 Fax 96 3540106

c/ Aparicio, 5 entlo. 5 - 03003 **Alicante**
Tfno. 96 5926583

Galicia
Avda. Gral. Sanjurjo, 119-1º dcha
15006 **A Coruña**
Tfno. 981 153969 Fax 881 927603

Castilla y León
c/ Caridad, 1 - 2º C - 47001 **Valladolid**
Tfno/Fax. 983 373173

Extremadura
c/ Camilo José Cela, 1 3º - 06800 **Mérida**
Tfno/Fax. 924 387468

c/ Gómez Becerra, 25 3º - 10001 **Cáceres**
Tfno/Fax. 927 626336

Andalucía
Av. Eduardo Dato, 85 1ºB - 41005 **Sevilla**
Tfno/Fax. 954 652434

c/ Salvador Noriega, 7 entreplanta dcha
29006 **Málaga**
Tfno/Fax. 952 088955

... o pregunte por nuestras delegaciones en otras provincias