PROYECTO INTERNACIONAL ADICAE

Medidas para la creación de un catálogo técnico europeo contra el fraude en medios de pago

Presentación y discusión de las propuestas técnicas contra el fraude de ADICAE

Comparativa legislación países, Actas Seminario Madrid, Anexo jurídico comparado

Organiza:

ADICAE
Asociación de Usuarios
de Bancos, Cajas y Seguros

Con la colaboración de:

Programa de Gestión de la Prevención, Preparación y Gestión del Terrorismo y otros Riesgos relativos a la Seguridad
Comisión Europea, Dirección General de Justicia, Libertad y Seguridad

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

A-S 200107

Indice

PRÓLOGO

Manuel Pardos:

Presidente de ADICAE, miembro del FSCG (Financial Services Consumer Group) y del FPEG (Fraud Prevention European Group) de la Comisión Europea, miembro del Consejo de Consumidores y Usuarios de España (CCU).

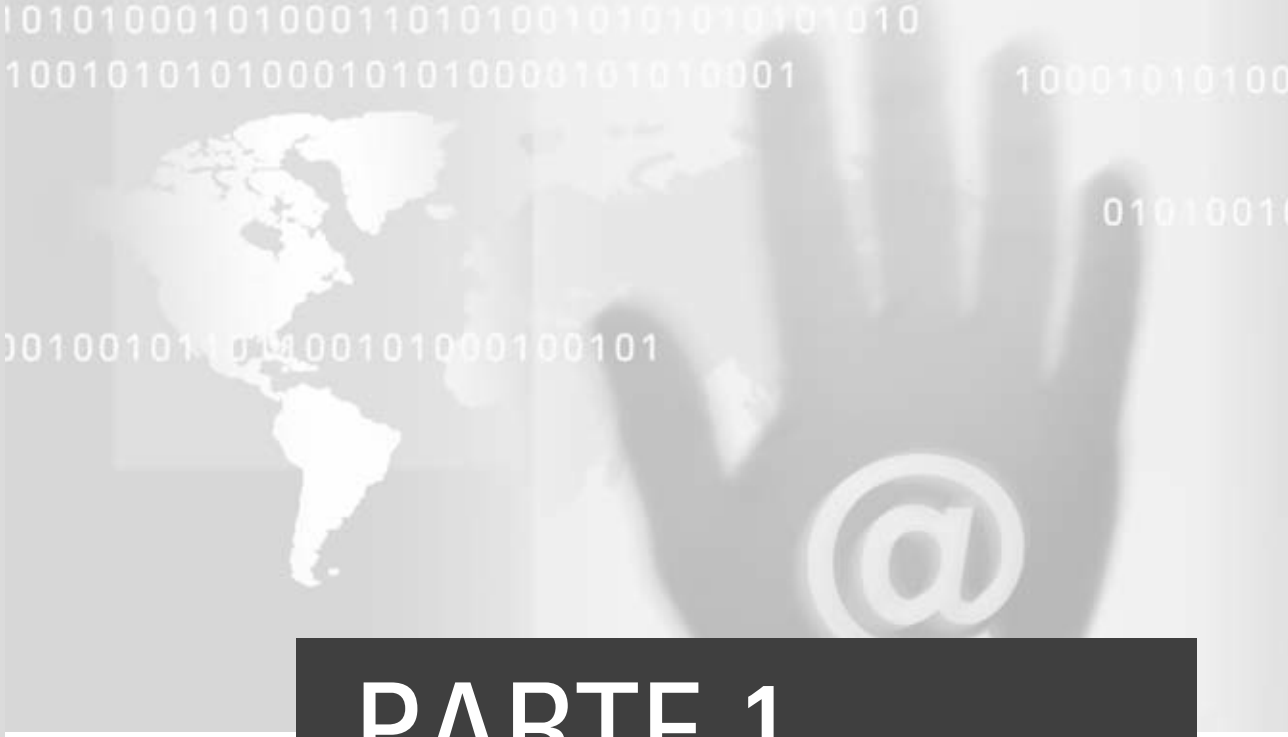
Tanto por su volumen como por su valor las operaciones efectuadas mediante instrumentos de pago electrónico representan un proporción cada vez mayor de los pagos dentro de la UE como fuera de ella. La tendencia indica que en los próximos años debido a los avances tecnológicos en los sistemas de pago electrónico su uso sea mucho más fácil por lo que está previsto que su uso se generalice aún más por parte de los consumidores.

La posibilidad de utilizar estos instrumentos en prácticamente todo el mundo exige que estos medios de pago sean eficaces, fáciles de usar, ampliamante aceptados, fiables y disponibles para la mayoría de la población europea. A parte de estas exigencias, es fundamental que un instrumento de pago generalizado y accesible para la mayoría de ciudadanos de la Unión Europea tenga las mayores medidas de seguridad posibles frente al fraude, tanto antes como después de la comisión de un delito. Ahí radicará la confianza de los consumidores en estos medios de pago alternativos al dinero en efectivo, y por ende su éxito y difusión.

Es preocupante el aumento del fraude en medios de pago durante estos últimos años, ligado también al aumento generalizado de su uso. Por ello, la difusión y carácter transnacional del fenómeno del fraude hacen necesaria la colaboración de todos los Estados y el diálogo entre los protagonistas del mundo de los medios de pago (entidades financieras, empresas de seguridad, emisores de tarjetas, consumidores, jueces, cuerpos policiales, etc) para la creación de una estrategia coherente de prevención a nivel europeo, toda vez que, a pesar de su eficacia, las medidas que han adoptado los Estados miembros hasta ahora no son suficientes para contrarrestar la amenaza que representa el fraude en los medios de pago en el presente y en el futuro más próximo.

Por ello, ADICAE desarrolló el proyecto "Creación de un catálogo europeo técnico del fraude a disposición de las autoridades judiciales y policiales en base a una red de alertas en información facilitada por entidades y ciudadanos" con el apoyo de la Comisión Europea y en el que colabora con otras asociaciones de consumidores europeas. Tras este proyecto queda como una conslusión general las evidentes insuficiencias en las políticas y estrategias de colaboración entre los países de la Unión Europea llevadas hasta ahora. Por ello sería necesarias la adopción de varias medidas, de las que tras las diversas ponencias y debates se tomó nota y se reflejan en la presente publicación. Entre las que hay que destacar la eliminación de malas prácticas y cláusulas abusivas en los contratos de medios de pago, en las que las entidades financieras se eximen de toda responsabilidad en caso de fraude; la aplicación de una serie de medidas como impulsar intercambios de información y colaboración entre instancias públicas y privadas; armonizar legislaciones nacionales en términos de prevención y represión; crear una base de datos coordinada por Europol con elementos susceptibles de fraude para la utilización por los diferentes organismos compententes en materia de persecución del fraude en cada uno de los estados de la Unión Europea, y la colaboración entre Asociaciones de consumidores de todas Europa y cuerpos policiales, administración de justicia, empresas del sector, entidades financieras, etc para emprender campañas informativas de gran difusión para concienciar y educar a los usuarios en la utilización de sus medios de pago.

Estas y otras conclusiones y propuestas que fueron expuestas en el Simposium Europeo "La crisis económica y el fraude en los medios de pago en España y la Unión Europea" han sido recogidas en esta publicación, que, desde ADICAE, pretendemos que sea un impulso más para la adopción de medidas y soluciones que pongan freno al fenómeno tan preocupante para los consumidores como es el fraude en sus medios de pago.



PARTE 1

Creación de un catálogo europeo técnico contra el fraude

Presentación del proyecto

PRESENTACIÓN DE PROYECTO EUROPEO

ADICAE, debido al alarmante aumento del fraude en medios de pago que sufren los consumidores y las perspectivas nada esperanzadoras para el futuro afrontó este proyecto europeo denominado "Creación de un catálogo europeo técnico del fraude a disposición de las autoridades judiciales y policiales en base a una red de alertas en información facilitada por entidades y ciudadanos" con el apoyo de la Comisión Europea y en el que colabora con otras Asociaciones de consumidores europeas.

OBJETIVOS DEL PROYECTO

Dentro del fraude financiero en la UE destaca por su repercusión en cientos de miles de usuarios y en la propia seguridad del sistema, el fraude en medios de pago distintos del efectivo, cuyas cifras actuales, y más aún su progresivo crecimiento previsible para los próximos años, hacen necesaria la adopción de medidas en todos los países, pero de manera especialmente intensa en los Estados de reciente incorporación a la Unión y en los candidatos a incorporarse en un futuro, donde las perspectivas de fraude derivadas de la progresiva extensión de los medios de pago, las inversiones y el crecimiento turístico (con el aumento de movilidad de ciudadanos de la Unión), configuran una situación de especial riesgo.

Los objetivos que se plantearon en este proyecto fueron:

- La cooperación de los ususarios y las víctimas a la reducción del fraude en medios de pago en los países partner.
- Incrementar el conocimiento de los responsables de las organizaciones representativas de los ususarios sobre tipos, mecanismos del fraude y formas de defensa.
- Favorecer el intercambio de información transnacional sobre el fraude, aumentando la coordinación y la cooperación entre los diferentes actores a nivel europeo. Coordinándose también las medidas tomadas como respuesta para que sean comunes en todos los países de la UE, atenuando así el riesgo, asegurando una gestión de la crisis provocada y una más rápida y común respuesta en el caso de delito transfronterizo.
- Promover la cooperación con las instituciones públicas responsables de la lucha contra el fraude. Lo que ayudaría a prevenir o reducir los riesgos vinculados del fraude.

PAÍSES PARTICIPANTES

ADICAE

Asociación de Usuarios de Bancos, Cajas y Seguros de España

Eslovenia: "Asociación (MIPOR)""

Eslovaquia: "Asociación nacional eslovaca de consumidores (ASC)""

Italia: "Associazione (FEDERCONSUMATORI)"

Lituania: "Lithuanian National Consumer Federation (LNCF)"

República Checa: "Sdružení českých spotřebitelů (SČS)"

Rumania: "Asociatia Nationala pentru Protectia Consumatorilor si Promovarea Programelor si Strategiilor din Romania (ANPCPPS)"

ACTIVIDADES DEL PROYECTO

Como actividades de difusión de los resultados y conclusiones tras meses de estudio e investigación, y para hacer llegar la información a autoridades judiciales y policiales por un lado, y a consumidores por otro se decidieron elaborar /organizar los diferentes materiales/actividades:

- Catálogo técnico.
- Página Web, con una red de alertas sobre fraude.
- Estudio sobre el impacto e influencia del fraude en los consumidores.
- Simposium Europeo.

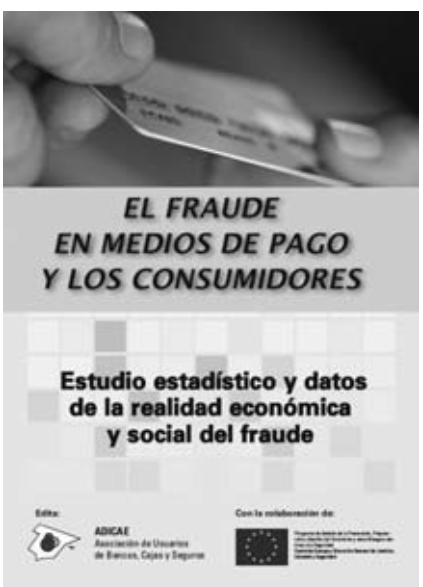
Catálogo Técnico: una herramienta para la formación y el debate

En particular, con esta publicación, piedra angular del resto de actividades y publicaciones del proyecto, se pretende concienciar y alertar a las autoridades judiciales y policiales de los riesgos que corren los ususarios de medios de pago, y a su vez, informar a los ususarios avanzados de cómo funcionan técnicamente sus medios de pago y cómo actúan los delincuentes aplicando las nuevas tecnologías para intentar engañarle. El objetivo que se persigue para cada uno de sus destinatarios era que las autoridades tomen medidas y soluciones de acuerdo a sus competencias y el usuario avanzado conozca en profundidad el fraude y sepa cómo evitarlo.

Además, como un objetivo ya anexo también se pretende que esta publicación sea una herramienta más de los operadores profesionales del mercado de medios de pago, administración de consumo, diversas instituciones económicas, etc como ampliación de puntos de vista y análisis del estado actual de los usuarios de medios de pago para un desarrollo más efectivo de su trabajo.

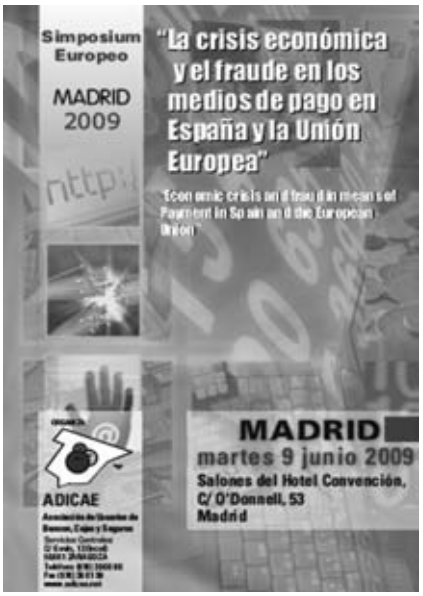
Estudio del impacto del fraude en los consumidores

Una de las inquetudes de ADICAE era dejar constancia del impacto que supone en las economías domésticas el fraude en medios de pago, cómo el fraude influye en los ususarios a la hora de utilizar sus tarjetas, banca electrónica, etc. Para ello se ha realizado un exhaustivo estudio de campo, obteniendo datos a través de los estudios recientes publicados por organizaciones, entidades y empresas especializadas en el tema del fraude en medios de pago y también con una encuesta realizada por ADICAE, tanto presencialmente como en la red, puesto que ésta ha estado a disposición de todo aquel que visitaba la web que se creó con motivo de este proyecto. Con todos estos datos y resultados se ha pretendido exponer la situación en la que se encuentran en este momento los consumidores, a la vez que proponer una soluciones lógicas y factibles a los actores del mundo de los medios de pago.

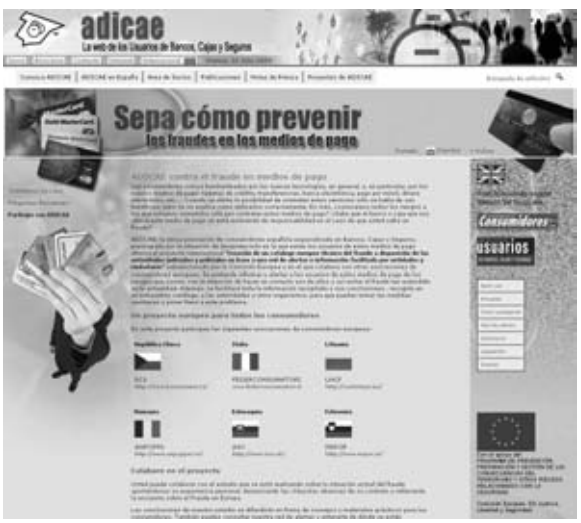


Simposium Europeo: puesta en común de problemas presentes y propuestas de solución futuras.

Como colofón al proyecto, en su último mes de vida, se organizó en Madrid el 9 de junio el Simposium Europeo "La crisis económica y el fraude en los medios de pago en España y la Unión Europea", y cuyos contenidos se reproducen en esta publicación. En él se dieron cita como ponentes y asistentes personalidades en el mundo del consumo en general y especialistas del mundo de la seguridad en medios de pago en particular. El objetivo era reunir a todos los protagonistas del mundo de medios de pago y que éstos expusiesen tanto su sensación y opinión sobre la situación del usuario de medios de pago ante el fraude y las posibles propuestas de solución a esta situación.



Pagina Web: Red de alertas (información y formación)



Otra de las publicaciones previstas en este proyecto y que ha utilizado la plataforma que ADICAE tienen en internet (www.adicae.net) ha sido la página web creada para tal ocasión. En ella se ha presentado el proyecto a todo sus visitantes, dandoles la oportunidad de conocer entre muchos contenidos qué tipos de fraude existen, un diccionario con los términos más frecuentes, consejos para evitar el fraude, una encuesta que pulsaba la opinión de los ususarios de medios de pago ante el fraude. Todos estos contenidos han supuesto un rotundo éxtio y que la página tenga un gran número de visitas.

No solo eso, sino que una parte importante de esta web la monopoliza la Red de alertas que ADICAE actualiza con periodicidad para alertar a los usuarios de los últimos fraudes detectados en este campo. Este medio no pretende estar activo durante la duración del proyecto, sino que la pretensión de ADICAE es ampliar y actualizar díariamente todo tipo de información que se produzca en este tema.

PARTE 2

Normativa de países de la U.E

Marco legislativo y particularidades

RUMANÍA

1. Marco legislativo general

Protección de los consumidores en la Constitución

Las leyes fundamentales rumanas no contienen estipulaciones especiales sobre protección del consumidor. Sin embargo, existen algunas disposiciones constitucionales que hacen referencia a la protección al ciudadano como consumidor.

El artículo número 135, línea 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 mención alguna sobre 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 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". 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 considerando la protección al consumidor. 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 el beneficio de una aplicación eficiente si están internacionalmente reconocidas (convenciones, tratos, 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).

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.

Normativa de los medios de pago según el Código Civil. Los contratos.

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 rumano contiene en el Libro III, Título III disposiciones que regulan los contratos. Entre estos, están las 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 acuerdo.

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; 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. Los vicios que afecten el consentimiento de las partes son: el error, la violencia y el dolo.

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 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 litigaciones 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. Particularidades de la Ley aplicable.

Los profesionales, considerando el 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 por correspondencia. Estas estipulaciones legales aluden a las condiciones de informar a los consumidores en los contractos 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.

Entre los derechos de los consumidores, los más importantes consideran lo siguiente:

- 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 tardea y una cláusula contrato será considerada abusiva.

- El derecho a la denuncia unilateral del contrato, con mención de las condiciones del consumidor de las que se hace uso.

Opuestamente a la normativa específica legal en materia de contratos de crédito, las siguientes situaciones fueron puestas en práctica:

- 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.

- La falta de una elaboración clara de los contratos.

- La falta de información con respecto al período de finalización, modos de ejecución, suspensión o paro del servicio: términos, notificaciones, condiciones del depósito, condiciones aseguradores.

Otras leyes aplicables:

■ 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.

REPÚBLICA CHECA

1. Marco legislativo general

La armonización del marco legal checo había sido completada con acervos relevantes hasta el 1 de mayo del 2004, la fecha de adhesión de la República Checa a la Unión Europea.

- 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. Particularidades de la Ley aplicable

A continuación, un resumen de algunas disposiciones legales contra fraudes en el área de pagos que no se efectúan en efectivo en la República Checa, 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 Conducto sobre los medios de pago.
- 97/7/EC: Directiva del Parlamente Europeo y la Comisión sobre la protección de los consumidores y contratos a distancia.
- 2001/413/EC: Resolución del marco del Consejo sobre combatir el fraude y la falsificación de medios de pago que no se efectúan en efectivo.
- 2000/31/EC: Resolución del marco del Consejo sobre 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.
- Transposición de cualquier decreto particular de la Comisión Europea debatidos a 97/489/EC: Recomendación de la Comisión, transacciones por pago electrónico.
- 87/598/EEC: Recomendación de la Comisión, Código europeo de Conducto sobre los medios de pago.
- 97/7/EC: Directiva del Parlamente Europeo y la Comisión sobre la protección de los consumidores y contratos a distancia.
- 2001/413/EC: Resolución del marco del Consejo sobre combatir el fraude y la falsificación de medios de pago que no se efectúan en efectivo.
- 2000/31/EC: Resolución del marco del Consejo sobre 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.

REPÚBLICA ESLOVACA

1. Marco legislativo general

Protección del consumidor en la Constitución

Aunque la Constitución Eslovaca fue establecida hace bastante años, en el 2002 (la República Eslovaca fue establecida después de separarse la antigua Checoslovaquia el 1 de enero del 2003) no se menciona a los consumidores.La Constitución no reconoce la categoría "Consumidor".

Constitución de la República Eslovaca

• 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.

Los medios de pago en el Código Civil

El Código Civil eslovaco está basado en el anterior Código Civil Checoslovaco 40/1964 que tiene numerosas novedades y cambios adoptados durante los últimos 44 años…

■ Norma civil (código 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
- Escritura de donación – párrafo 628 - 630
- Contrato de trabajo – párrafo 631 – 651
- Contrato para reparación y cambio – párrafo 652 – 656
- Contrato de préstamo – párrafo 657 – 662
- Contrato de arrendamiento – párrafo 663 – 723
- Contrato de recaudación – párrafo 724 – 741
- Contrato de alojamiento – párrafo 754 – 759
- Contrato de transporte – párrafo 760 – 773
- Contrato de comisión – párrafo 774 – 777
- Contrato de seguro – párrafo 788 – 828

■ Norma de consumo (código de normas de consumo o similares)
- Decreto del consumidor 250/2007 efectivo desde el 1 de julio del 2007
- Derechos del consumidor – párrafo 3
- Obligaciones de información – párrafo 11 – 18

2. Particularidades de la Ley aplicable.

En cuanto a los pagos en efectivo hicieron esfuerzos 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 pero no fue efectivo y es incluso muy normal que se efectúen pagos de grandes cantidades con dinero en metálico.

Tarjetas 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. Artículo 25 – obligaciones y reclamaciones del consumidor contra el banco / emisor de tarjetas en casos de mal uso de la tarjeta.

Código Penal número 300/2005, artículo 219 – Falsificación y uso no autorizado de un medio de pago electrónico y una tarjeta de pago de otro – la pena básica es de 1 a 5 años de prisión y de 5 a 12 años en casos especiales – gran daño, como 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 información de identificación de una tarjeta sea mal usada y un consumidor se viese perjudicado por una retirada ilegal de dinero de su cuenta bancaria. En la mayoría de los casos los bancos / 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 en casos donde se desconoce al autor del fraude, lo que es muy común.

Transferencias

El decreto de Sistemas de pago número 510/2002, efectivo desde el 31 de agosto del 2002, artículos 3 al 11 para transferencias nacionales y arts. 12 al 20 para transferencias internacionales. No se identificó ninguna provisión específica para los Consumidores.

Cheques

No se identificó ninguna provisión específica para 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, arts. 21 al 24.

ESLOVENIA

1. Marco legislativo general

Protección de los consumidores en la Constitución

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.

Normativa de los medios de pago según el Código Civil

El cuerpo principal de la ley en este campo no es el Código Civil, sino el Código de las obligaciones. Se encontrarán más especificaciones en la Ley de protección al consumidor y en la Ley de los medios de pago.

- Código de obligaciones
  - 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

- Ley de protección del consumidor:
  - Art. 23-24: Prohibición de términos contractuales desleales
  - Art. 45: Diligencia de los mensajes publicitarios no deseados

- 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 comunicación electrónica
  - Art. 109: diligencia de los mensajes publicitarios no deseados

- Ley de la banca:
  - Art. 230: Resolución de disputas entre bancos y consumidores

- Ley de protección de datos, en relación con los artículos del Codigo 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

2. Particularidades de la Ley aplicable

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.

País	Legislación penal sobre fraude
Rep. Checa	Sí (Código Penal , 140/1961)
Italia	Código Penal: Sección 491: Falsificación de documentos electrónicos; Section 635-bis: Daños a las redes informáticas y de telecomunicaciones; Section 615: Difusión de virus y malware; Sección 392: Daños a la propiedad (incluidos bienes electrónicos); Section 494: Robo de personalidad.
Lituania	Sí
Rumanía	Sí
Eslovenia	Código Penal: Art 154 (Mal uso de datos personales); Art 225: Acceso no autorizado a sistemas informáticos; Art. 242: Invasión de sistemas de información; Art 309: Producción y adquisición de herramientas para la realización de actos penados.
Rep. Eslovaca	Código Penal nº300/2005, § 219 - Falsificación y uso no autorizado de medios de pago electrónicos y tarjetas de pago.

BULGARIA

1. Marco legislativo general

Protección de los consumidores en la Constitución

El artículo 19 de la Constitución, economía libre de mercado, basada en la iniciativa libre, donde la ley garantiza condiciones igualitarias para la actividad económica a las entidades individuales y legales protegiendo los derechos de los consumidores, luchando contra la competencia desleal y las prácticas de monopolio.

Normativa de los medios de pago según el Código Civil.

Los medios de pago se regulan como mínimo por varios decretos, llamados 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. Particularidades de la Ley aplicable

Tarjetas de crédito

La normativa que regula las tarjetas es:

• 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. Afirma 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.

Transferencias, cheques y pagos on-line

Los artículos 27 a 40 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.

País	Legislación civil sobre fraude
Rep. Checa	Código Civil no. 40/1964, Código de Comercio no. 13/1991, etc.
Italia	Ley 197/1991, sección 12 (Uso indebido de tarjetas de crédito), Ley de Protección de Datos, sección 34 (2003), Ley del Cheque, Ley sobre el Fraude Informático (547/2003), Decreto n. 112 (30 April 2007): Creación de un Sistema de Prevención del Fraude en Tarjetas de Crédito.
Lituania	Ley Bancaria (2004): Art 56; Ley de Transferencias (1999) Medios de Pago Electrónicos, Ley del Cheque (1999) y Artículo 1104 del Código Civil (Regulación mecanismo cheque), Ley de Contratación a distancia (2001): Art. 7, 11, 12, 14, 16 y 23; Código Civil (Art. 6366, 6367)
Rumanía	Comercio Electrónico (365/2002), Protección datos personales (677/2001), Firma Electrónica (455/2001), Medios de Pago a Distancia (Regulación 4/2000 del Banco Nacional de Rumanía)
Eslovenia	Ley de Medios de Pago (Art. 9, 13, 24) ; Ley Bancaria (Art. 230), Ley del Cheque.
Rep. Eslovaca	Uso insebido de tarjetas de crédito (Ley 510/2002, § 25)

ITALIA

1. Marco legislativo general

Protección de los consumidores 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

La 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 uno no puede 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 privatto (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. Particularidades de la Ley aplicable.

Tarjetas 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 significativo 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 límí-

tes. En lo referente a este problema, por favor, diríjase a la referencia posterior en la sección "Pagos en línea".

Transferencia

No existen estatutos concretos o jurisprudencia relativos a las transferencias.

Cheques

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 referencia a consumidores.

Pagos en línea

Supone que el pago, estrictamente conectado a la tecnología de la información, podría dar origen a los llamados "delitos informáticos". ¿Cómo se enfrenta a este tipo de 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.

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 provistos 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 intercepción, 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 cibeméticos, 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.

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).

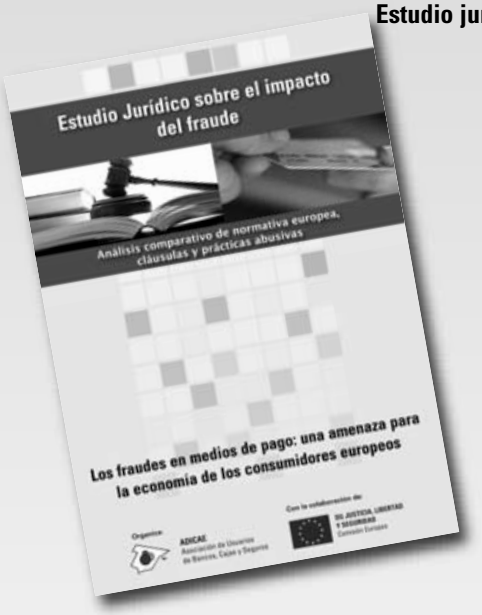
Esto también podría responder al análisis económico de los criterios de la ley, según la que los daños deben recaer, en parte o en su totalidad, en el actor económico que tiene la parte de beneficios más grande en esa actividad concreta (por ejemplo, el emisor de la tarjeta o el banquero electrónico).

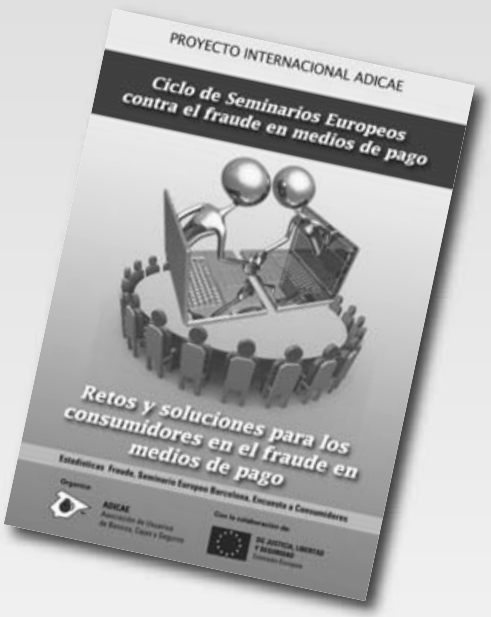
De este modo, la responsabilidad cambiaría, en parte o en su totalidad, de la víctima del crimen cibernético a las compañías que operan en el sector. Aunque podríamos apreciar y estamos de acuerdo en esa sugerencia, las leyes civiles aplicables existentes ofrecen muy pocas pistas para la investigación de una solución previsible.

PUBLICACIONES PROYECTO "CICLO DE SEMINARIOS EUROPEOS"

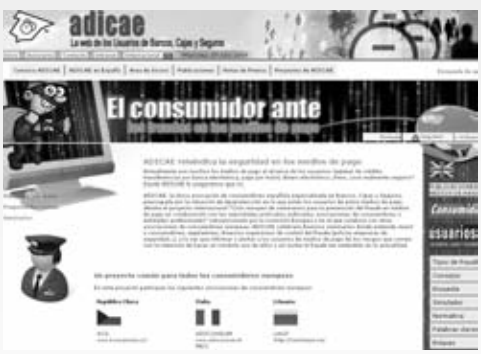
Si quiere conocer más solicite las publicaciones del otro Proyecto europeo sobre el fraude en medios de pago de ADICAE

Estudio jurídico sobre el fraude

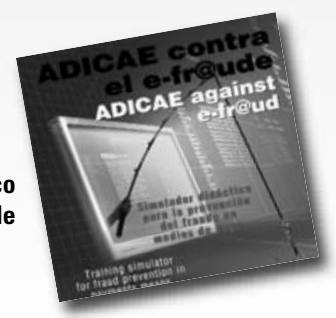




Libro seminario internacional del proyecto



Página web del proyecto



Simulador informático contra el fraude

PARTE 3

La Crisis económica y el fraude en los medios de pago en España y la U.E.

Debate sobre los problemas y sus soluciones

ACTO DE APERTURA

■ **D. Manuel Pardos**
Presidente de ADICAE

El uso de los de medios de pago electrónico, ya no es una novedad, desde hace años la mayoría de los países europeos paga con tarjeta a gran escala, incrementandose año a año el número de operaciones y el volumen de dinero que se pone en movimiento con medios de pago que no son el efectivo. España, como se va a ver a lo largo de las diferentes ponencias, es un claro ejemplo de este aumento del uso de estos medios de pago. El "dinero de plástico" es un medio que se ha generalizado y universalizado para la mayoría de los ciudadanos, son los jóvenes e incluso los niños (siempre con limitaciones y el control de sus padres), los que empiezan a utilizar estos medios de pago con bastante familiaridad. Además, se ha dado un paso de gigante con internet, con la cada vez mayor utilización de este medio para realizar compras y efectuar pagos y transacciones.

A todo ello, hay que sumar el fenómeno del teléfono móvil. Éste no podía ser ajeno, y a parte de sus diferentes utilidades y aplicaciones se ha visto en este una función más: su uso como medio de pago. Aunque también hay que decir que éste de momento no está generalizado, pero se prevé que su uso en el futuro sea el líder de los medios de pago.

A esta situación hay que añadir factores tales como la crisis económica que está incrementando el volumen de comercio electrónico y el número de operaciones por la vía de internet debido al abaratamiento de costes y servicios a parte del avance de las nuevas tecnologías.

Todo ello hace que se dé paso a nuevas formas de desarrollo, pero en este panorama también ha progresado geométricamente el fraude. Por ello, las autoridades europeas y nacionales de los países de la UE han mostrado su preocupación ante este fenómeno del fraude creciente en los medios de pago electrónicos. El objetivo mínimo de estas autoridades es la reducción del fenómeno adjetivo y no sustancial del fraude en estos medios.

Se debe tomar muy en cuenta la confianza de los consumidores en sus medios de pago, y cómo el fraude influye negativamente en ésta. En consecuencia, las asociaciones de consumidores debemos propagar la confianza en estos medios mediante la defensa de los consumidores, no solo a la hora de informarles para protegerse de los efectos y consecuencias del fraude, sino también propugnando que este cambio de tendencia en la utilización del dinero en efectivo hacia el dinero "de plástico" sea mucho más barato. Se deben abaratar costes y comisiones en los medios de pago más utilizados, debe existir facilidad en su acceso, en su utilización y, logicamente, mejorar su seguridad. La confianza se reforzará con el afianzamiento de los pilares anteriores. En definitiva, previa a la confianza de éstos viene la protección de sus derechos y la seguridad en su uso.

Para el reforzamiento de la confianza de los ususarios de medios de pago es necesario que las entidades financieras garanticen la seguridad de estos medios y que la carga de la prueba, en caso de fraude, corresponda a la entidad. El

consumidor sólo debe responder cuando sea claramente negligente en el uso de sus medios de pago. Es necesario que las entidades financieras cumplan la Recomendación de la Comisión europea de 1988 que las Asociaciones Europeas de Bancos y de Cajas de Ahorros aceptaron cumplir en 1.990, y por la que la responsabilidad del titular de tarjeta por utilización fraudulenta tras robo, quedó fijada en 150 euros: límite máximo de responsabilidad del consumidor hasta el momento de la notificación del robo o perdida de la tarjeta.

En este aspecto es importante una mayor preocupación por parte de las entidades y que se muestren interesadas por la opinión de los ususarios de los medios de pago. Digo esto por que después de muchos esfuerzos e interés por parte de ADICAE en que las entidades financieras estén presentes trasladándoles la invitación a participar activamente en las diversas ponencias sólo se ha conseguido la presencia de una de ellas.

Para concluir, decir que es necesaria la colaboración entre todos los actores del mundo de los medios de pago, es fundamental que primero primen los intereses colectivos, incluidos los de los usuarios, y queden aparcados los meros intereses económicos y competitivos entre empresas.

■ Dña. Francisca Sauquillo

Presidenta del Consejo de Consumidores y Usuarios de España

Es preocupante el fenómeno del fraude, puesto que siempre ha existido pero en la actualidad ha evolucionado hasta unos límites que hacen que todos trabajemos para frenar su avance. De ahí la importancia de un proyecto transfronterizo de gran relieve para reunirse y valorar el trabajo hecho y el trabajo que queda por hacer. Es necesario informar, formar (mediante actos como este seminario) y aprender de las experiencias de los distintos países, para así valorar las diferentes soluciones y alternativas que se pueden plantear para hacer frente al fraude en medios de pago.

Este problema gracias a las nuevas tecnologías se ha globalizado y generalizado, por lo que a este problema mundial y global hay que ponerle soluciones globales. No es el problema de unos, sino el de todos. Debemos evitar este individualismo al que se ha llegado en materia de consumo. Por eso es necesario que al igual que se propagan como mucha facilidad los fraudes también hay que hacer circular la información sobre estos. Cuanta más información se tenga sobre los nuevos fenómenos de fraude, mayor conocimiento y armas preventivas contra éstos puede haber. De ahí la necesidad de utilizar sistemas de alerta eficaces para que los consumidores y usuarios sepan detectar el fraude.

Es un seminario muy oportuno con la nueva Europa, en la que se da una nueva situación de poder legislar, con la incorporación de nuevos países, con los mismos problemas globales pero también con problemas particulares. Por eso, es importante la labor del legislador y de las diferentes comisiones de elaboración de normativa, que tienen que estar atentas a la evolución del fenómeno del fraude para poder proponer normativa cada vez más homogénea, que sea común a un problema común que sufren todos los consumidores europeos, ya que quienes cometen fraudes van muy adelantados y nosotros debemos, en esta carrera, procurar ganar, intentar prever el futuro para que los delincuentes no consigan su objetivo.

RETOS Y DEFICIENCIAS DE LA NORMATIVA EN LA PROTECCIÓN AL CONSUMIDOR ANTE EL FRAUDE EN MEDIOS DE PAGO.

■ **Dña. Delia Vaquerizo**

Gerente Responsable del Área de Productos y Servicios del Sistema 4B

En la sociedad actual, dentro del contexto de la Unión Europea, los Medios de Pago electrónicos se han convertido en una herramienta imprescindible para la gran mayoría de los usuarios de banca, tanto para el pago en comercios, como para la disposición de efectivo en comercios. Resulta difícil imaginar un mundo sin tarjetas financieras. En este escenario, es esencial mantener la estabilidad del sistema. El control del fraude en los Medios de Pago es uno de los factores que más deben tenerse en cuenta por el impacto que provocan en la confianza del usuario. La globalización, la movilidad de los usuarios y la potencial vulnerabilidad de los datos personales a través de Internet y otros canales, han favorecido la aparición de mafias organizadas a escala mundial dedicadas a la falsificación y uso fraudulento de las tarjetas financieras

Nuevos métodos contra la lucha contra el fraude

Las entidades financieras españolas son conscientes de esta situación y emplean grandes esfuerzos y recursos para prevenir y evitar el fraude. Como prueba de ese esfuerzo, las tres redes de tarjetas españolas: Servired, Euro6000 y Sistema 4B presentan niveles de fraude muy inferiores a la media europea, por debajo del 0.04% sobre el total de las ventas.

Sin embargo, en la lucha contra el fraude deben participar coordinadamente todos los agentes implicados enfocando sus acciones en torno a cuatro conceptos básicos:

- Prevención.
- Detección
- Detención
- Análisis y control.

Los Esquemas de pago y las entidades financieras trabajan activamente con la Administración en la definición de estándares de seguridad y requerimientos de control que optimicen el uso de los Medios de Pago. De este modo, para minimizar el riesgo de falsificación del plástico físico, se ha establecido como estándar europeo la tarjeta EMV, que incorpora un sofisticado chip con elevados niveles de seguridad en la verificación del titular. En España se ha iniciado ya el proceso de migración.

En los países europeos donde la migración a EMV está en fases muy avanzadas, se ha demostrado la eficacia en la reducción del fraude presencial recogido en Europa, si bien, se ha identificado un desplazamiento de los delincuentes a las zonas del mundo donde aún no se reconoce el estándar EMV (Asia y América principalmente).

Asimismo, el nuevo estándar no protege contra el fraude en comercio electrónico y venta a distancia., que está experimentando un crecimiento en línea con el incremento de la actividad en este canal.

Para proteger al titular de tarjeta que compra en Internet, existe un estándar de seguridad (3D secure) que certifica al usuario ante su entidad financiera para el pago a través de Internet . Los comercios calificados como “Seguros”, solicitarán al titular de la tarjeta que utilice su certificado para verificar su identidad y autorizar la operación. Para obtener este certificado, el usuario debe contactar con el banco emisor de su tarjeta, normalmente a través de su página WEB. Debe ser una iniciativa voluntaria del usuario. Normalmente la entidad financiera puede hacer campañas promocionales o informativas, pero el alta del certificado deberá ser iniciada siempre por el titular. Los comercios que no solicitan este certificado son calificados como “No seguros” y deben aceptar el retroceso de la operación en caso de que se denuncie como falsa por el titular.

En el caso de la venta a distancia, el usuario debe informar del código de tres dígitos que aparece impreso en la parte derecha del panel de firma, para ratificar que esté en posesión de la tarjeta. Este número no debe ser cedido por escrito o por teléfono para ningún otro fin que no sea una operación de compra.

¿Cómo evitar la comisión del delito?: Medidas de prevención.

Otra gran preocupación de las entidades es dónde y cómo se copian las tarjetas. En muchos casos, la copia se realiza en un cajero al que se le ha instalado un dispositivo para el copiado de tarjetas. Los bancos europeos han publicado recientemente un conjunto de recomendaciones para las entidades propietarias de cajeros automáticos, encaminadas a aumentar su seguridad y reducir el riesgo de ataques de este tipo. En el caso de Sistema 4B estas prácticas se aplican como norma para mejorar la seguridad de la red TELEBANCO 4B. No obstante, si el usuario identifica algún elemento extraño en el cajero, debe informar cuanto antes sobre ello a su entidad o a Sistema 4B directamente en el caso de cajeros de esta red.

A pesar de estos controles preventivos, Sistema 4B y el resto de esquemas de pago nacionales, monitorizan la actividad de las tarjetas a través de sistemas inteligentes para identificar conductas sospechosas indicativas de fraude. Si existe sospecha de fraude se intenta contactar con el titular para alertarle o asegurar que no existe riesgo. Si no es posible contactar con el titular pero el riesgo de fraude es muy alto, la tarjeta puede ser temporalmente bloqueada para evitar que se produzca quebranto económico. Aunque en ocasiones esto puede suponer un trastorno para el cliente, se entiende como un mal menor para defender sus intereses.

Muchas entidades financieras ofertan a sus clientes un servicio complementario de información transaccional por SMS que es de gran utilidad para le reducción del fraude. La experiencia de las entidades de Sistema 4B que han habilitado este servicio para sus clientes es muy positiva, con reducciones de hasta un 40% en el importe de fraude.

A pesar de todas las medidas descritas, el fraude puede llegar a producirse. La denuncia inmediata y rigurosa del fraude por parte de la víctima, tanto a las Fuerzas y Cuerpos de Seguridad del Estado como a su entidad financiera, son esenciales para facilitar la identificación de los delincuentes, su ubicación y sus patrones de comportamiento, que serán trasladados por las Entidades financieras a sus sistemas inteligentes de prevención. El usuario debe vigilar con regularidad su estado de cuentas para identificar lo antes posible actividad fraudulenta de su tarjeta. Desde el momento que notifique a su entidad que ha sido víctima de un fraude o robo, ésta se hará cargo de todo el quebranto económico. Además, la nueva Directiva europea para los Medios de Pago, al objeto de aumentar la protección del titular, cifra en 150 euros la franquicia a partir de la cual se traslada a la entidad financiera el importe del fraude.

Acciones y medidas de prevención, detección y análisis de la información:

- Procedimientos seguros de emisión y distribución de tarjetas y número secreto
- Emisión y distribución de tarjetas desactivadas para la activación por el titular con procedimientos de autenticación del mismo.
- Control de marcas internas y aleatorias que se actualizan en cada operación y que permiten identificar con rapidez si una tarjeta ha sido falsificada.
- Control y actualización permanente de listas negras de tarjetas bloqueadas por robo, pérdida o falsificación para que no puedan volver a ser utilizadas.
- .• Monitorización de las transacciones casi en tiempo real contra sistemas inteligentes de patrones de fraude, que alertan sobre alteraciones en la conducta de la tarjeta. Así se detectan posibles anomalías yse le notifican al titular.
- Notificación (opcional) vía SMS de las transacciones realizadas para el control del titular.
- Análisis permanente de los expedientes de fraude de todas las entidades miembro para la identificación de patrones comunes de fraude con los que entrenar a los sistemas de monitorización y alerta.
- Análisis histórico de la actividad de las tarjetas para la identificación de los puntos de copia. Procedimientos de actuación preventiva contra las tarjetas potencialmente falsificadas. Éste es un procedimiento de actuación preventivo.
- Certificación y activación de políticas de implantación de terminales seguros, es decir, cajeros y puntos de venta que no puedan ser manipulados para la copia de tarjetas(skimming).
- Cumplimiento de todos los estándares PCI (Payment Card Industry) para la protección y confidencialidad de los datos procesados.

Conclusiones y propuestas para evitar el fraude

En definitiva, la lucha contra el fraude en los medios de pago se ha convertido en los últimos años, en una prioridad para las entidades financieras, los reguladores y los procesadores, conscientes del impacto que la desconfianza ante un posible fraude puede tener en el uso de las tarjetas. Todos los intervinientes en el sistema son esenciales para el control del fraude y la protección del usuario y del Sistema:

■ Los usuarios, siguiendo las buenas prácticas y las recomendaciones de uso seguro de las tarjetas financieras.

■ Los comercios, respetando la operativa establecida, solicitando la autenticación del titular y denunciando inmediatamente cualquier comportamiento sospechoso.

■ Los Esquemas de Pago, las entidades financieras y los procesadores, así como los organismos reguladores, definiendo y actualizando las políticas de protección de fraude, vigilando la aplicación de los estándares de seguridad establecidos, compartiendo información sobre fraude y participando activamente en la definición de nuevos estándares y mecanismos de protección. En este sentido, Sistema 4B potencia el intercambio de información relativa al fraude y comparte los avanes que pueda realizar en este campo tanto a nivel nacional como internacional a través de su participación en instituciones dedicadas a la lucha contra el fraude.

■ La Policía, apoyándose en la información aportada por los esquemas y los bancos y colaborando con el resto de cuerpos de Seguridad nacionales y extranjeros.

■ La Fiscalía, exigiendo el máximo rigor en la cumplimentación de expedientes.

Los medios de pago son y deben seguir siendo un servicio seguro para el usuario de banca como medio de acceso a su dinero. El usuario debe saber que está protegido ante el fraude porque se minimiza el riesgo con medidas preventivas y se limita la responsabilidad en caso de que ocurra.

■ **Dña. Daniela Bulcu**

Fiscal Jefe del Ministerio de Jusicia de Rumanía

La aparición de los primeros ordenadores hace más de 50 años inició una revolución real para la sociedad. La primera consecuencia principal de la mejora tecnológica fue representada por la transición de la sociedad industrial a la sociedad de la información. La humanidad ha conocido una evolución grande en este tiempo. Como herramienta tecnológica en continua mejora, el ordenador se ha convertido en un componente normal de nuestras vidas, y está presente en todos los aspectos de la vida económica, social y cultural.

El desarrollo tecnológico y el uso a gran escala de sistemas informáticos tiene ventajas pero también riesgos. La dependencia de los agentes económicos, instituciones públicas y usuarios individuales de sistemas informáticos les hace más y más vulnerables al impacto del crimen informático. Los ordenadores también han sido una atracción para aquellas personas que vieron una manera de conseguir ventajas inmerecidas. Así, los ordenadores fueron primero utilizados para cometer delitos pequeños, y más tarde para realizar algunas formas nuevas de delitos ilícitos, más adelantados y específicos del ámbito informático.

El cibercrimen, un fenómeno actual

La criminalidad informática es un fenómeno de nuestros días, cada vez más conocido debido al hecho que se ha extendido muy rápidamente también en cuanto a sus consecuencias desde el punto de vista económico y social. Un estudio ha mostrado que el miedo de las personas a los ataques informáticos es más alto que el que tienen a otro tipo de fraudes o robos menores. La búsqueda criminal de los delitos cometidos en el terreno de los sistemas informáticos está todavía en proceso de mejora, debido a que sólo una parte pequeña de los delitos que implican sistemas informáticos son conocidos por los organismos de búsqueda penal.

Pese a que hoy es posible hacer una descripción del tipo de los delitos cometidos en el terreno informático, es todavía muy difícil de hacer una síntesis de las pérdidas causadas por estos delitos, así como también del número exacto de delitos cometidos. Durante 2003 los servicios especializados en Rumanía han investigado unos 200 delitos informáticos, el 50% de ellos relacionados subastas electrónicas fraudulentas, el 30% relacionados con órdenes on-line fraudulentas, el 10 % implicados en el acceso no autorizado a sistemas informáticos y el 10% relacionados con la pornografía infantil.

Incorporación de Rumanía a la UE: consecuencias en la regulación contra el fraude

Partiendo de la premisa que la criminalidad informática puede causar muchos problemas dentro de la sociedad moderna, Rumanía ha aplicado a su sistema legal la legislación con respecto la criminalidad informática que corresponde a las convenciones y estándares internacionales. Así, para trasponer a la legislación nacional las obligaciones supuestas como país miembro, Rumanía ha ratificado con la Ley no. 64/2004 la Convención con respecto a la criminalidad informática adoptada por el Consejo de Europa en Budapest en 2001. Nuestro país también ha estado de acuerdo con la Recomendación no. R/95/13 del Comité de Ministerios, que tuvo lugar el 11 septiembre de 1995, con respecto a los problemas en el procedimiento criminal relacionado con tecnologías informativas.

Así, para cumplir con la Unión Europea, Rumanía adoptó leyes nuevas, como la Ley 365/2002 respecto al comercio electrónico. En el artículo 2 de esta ley se define el propósito y el campo de aplicación de esta ley. Por las disposiciones de los artículos 24-28 las siguientes acciones son castigadas: la falsificación de medios electrónicos de pago, la posesión de equipos con el propósito de falsificar tales instrumentos, falsas declaraciones para emitir y utilizar medios electrónicos de pago, hacer operaciones financieras de una manera fraudulenta, aceptar las operaciones financieras hechas de una manera fraudulenta. Estos delitos son castigados con prisión de 1 a 12 años. Estos dos actos normativos completan las provisiones de Ley 39/2003 con respecto a la prevención y lucha contra la criminalidad organizada y Ley no. 21/1999 sobre la prevención y la lucha contra el blanqueo de dinero. En 2003 fue adoptada la ley no. 16 con respecto a la prevención y la lucha contra la criminalidad informática. El delito informático es definido por el art. 49 de esta ley como el acto de causar un prejuicio a una persona por introducir, cambiar o eliminar datos informáticos, por restringir el acceso a esos datos o por impedir el funcionamiento de un sistema informático, con el propósito de obtener un beneficio material para él o para otro. Es delito es castigado con prisión de 3 a 12 años. La víctima puede ser una persona o una empresa que vea afectado su propio sistema informático. Hay que matizar que la mera intención también es castigada en esta normativa.

Tendencias de futuro de los delitos informáticos: soluciones de la Administración de Justicia en Rumanía

Del análisis de los datos de la criminalidad informática podemos observar las tendencias futuras de estos delitos, tendencias que representan límites nuevos para quienes organizan actividades para proteger el consumidor (como autoridades, empresas, analistas, asociaciones de consumidores).

Así, los delitos informáticos afectan directamente a la sociedad, puesto que ésta depende cada vez más de los ordenadores. Los componentes importantes de nuestra vida social son coordinados por redes y sistemas informáticos. Como consecuencia, los ataques mediante ordenadores y hacia los ordenadores se multiplicarán en el futuro. A esto hay que sumar que los delitos informáticos pueden ser cometidos virtualmente por cualquier persona, puesto que los sistemas informáticos son accesibles para la mayoría de la población debido a sus bajos precios, y pueden afectar a miles y miles de personas en cualquier parte del mundo (globalización del fraude).

Para hacer frente al problema de los delitos informáticos, la institución que represento, que es la OFICINA DEL FISCAL sujeta al TRIBUNAL SUPREMO DE CASACIÓN Y JUSTICIA, el departamento especializado del Ministerio de Comunicaciones y Tecnología de la Información y el Departamento de Lucha contra la Criminalidad Informática dentro del Ministerio de Defensa, ha creado el portal de Internet "eFraude" que permite que cualquiera que esté interesado pueda dejar una denuncia a las autoridades ante un posible fraude u otras actividades ilegales en internet.

Cooperación internacional

Debido al anonimato que ofrecen, la posibilidad de enviar mensajes encriptados, y debido a su carácter transnacional, la cantidad de información no puede ser controlada, y es por eso que los delitos informáticos son los preferidos por los defraudadores. En este sentido, Rumanía es muy activa en el campo de la cooperación internacional para emprender este problema. La Ley 16/2003 estipula en Capítulo V referente a la cooperación internacional que las autoridades judiciales rumanas cooperen, de acuerdo con las provisiones de ley y en conformidad con los instrumentos jurídicos internacionales de los que Rumanía también es parte, con las instituciones similares formadas en otros estados y con organizaciones internacionales en el área.

Para asegurar que la cooperación internacional sea inmediata y permanente en el área de luchar contra los delitos informáticos, existe un punto de contacto permanente - Servicio para luchar contra los delitos informáticos- dentro de la Dirección para la Investigación de Delitos Organizados y Terrorismo. DIICOT ha sido creado por la Ley 508/2005 y es la estructura única dentro del Ministerio Público especializada en luchar e investigar ofensas de terrorismo y delito organizado. Ha sido creado para desintegrar o marginar a los grupos organizados nacionales de las barreras fronterizas, los cuales cometen delitos graves.

Dentro de la cooperación internacional, las autoridades extranjeras pueden pedir a este servicio la conservación inmediata de datos informáticos o datos referidos al tráfico informático que existen en un sistema informático dentro del territorio rumano. Para esto la autoridad extranjera tiene que formular una petición de asistencia judicial internacional en ley criminal. A la vez, las autoridades rumanas pueden transmitir a autoridades extranjeras competentes información y datos que posean que puedan ser necesarios para descubrir los delitos cometidos por sistemas informáticos o que son necesarios para solucionar casos referidos a estos delitos.

En lo referente a la Ley 161/2003 para la prevención de delitos informáticos incluye algunos artículos que estipulan que autoridades e instituciones públicas tienen competencias en esta área, proveedores de servicios, asociaciones de protección de los consumidores y otros representantes de la sociedad civil que desarrollan actividades de prevención y programas para luchar contra los delitos informáticos. Todas estas entidades organizan campañas de información respecto a los delitos informáticos y los riesgos implicados para los usuarios de sistemas informáticos.

En Rumanía el Ministerio de Justicia en cooperación con el Ministerio de Administración e Interior y el Ministerio de Comunicaciones y Tecnología de la Información desarrolla y actualiza permanentemente una base de datos respecto a los delitos informáticos. A si vez. dirigen periódicamente estudios para identificar las causas y condiciones que favorecen el fraude y los delitos informáticos.

Conclusiones y propuestas para evitar el fraude

Considero que tendría que haber un equilibrio entre legislación y realidades sociales en este área, ya que en estos momento no se corresponden la una con la otra. De ahí que para que la legislación fuese eficaz en la protección de los ciudadanos, su adaptación a la realidad tendría que ser lo más rápida posible. Es necesario que los procedimientos de elaboración y aprobación de normativa sean mucho más dinámicos y rápidos, para estar lo más proximos a la realidad y regularla con efectividad.

Además los representantes de la sociedad civil y asociaciones de protección de los consumidores tienen una función muy importante en educar a la población sobre los riesgos a los que son expuestos. Las asociaciones de consumidores deben animar a las victimas de delitos informáticos a informar a las autoridades competentes sobre estos delitos. Como mencioné anteriormente muchos de estos delitos quedan sin revelar porque las víctimas no los denuncian a las autoridades competentes, con lo que estos quedan sin ser perseguidos y por lo tanto impunes.

LUCHA CONTRA LOS NUEVOS TIPOS DE FRAUDE ECONÓMICO Y FINANCIERO

■ **Dña. Nieves Gamoneda**

Inspectora de la Unidad Central de Delincuencia Económica y Fiscal - COMISARÍA GENERAL DE POLICÍA JUDICIAL (CUERPO NACIONAL DE POLICIA)

B.I.T.: Unidad especializada. Sus funciones

La seguridad pública es un derecho que debe garantizarse en cualquier entorno social, también en la Red. De ahí la existencia de la Brigada de Investigación Tecnológica (BIT) que es la Unidad policial destinada a responder los retos que plantean las nuevas formas de delincuencia, tales como pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería... Su misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial.

Las funciones básicas del BIT son la realización directa de investigaciones especialmente complejas, la coordinacion de operaciones que involucren a diversas Jefaturas Superiores, la formación del personal del cuerpo nacional de policia y otros miembros de policías extranjeras y la representación internacional y ejecución y coordinación de las investigaciones que tengan su origen en otros paises.

Especialización y división en secciones

La B.I.T. está dividida en tres secciones, 2 operativas y una técnica. Por un lado, una de las secciones operativas, está dedicada a la investigación en tres sectores, y que son los siguientes:

■ PROTECCIÓN AL MENOR, En cuanto a delitos contra menores, pornografía infantil y mas en concreto a la producción pornografica infantil.

■ FRAUDE A LAS TELECOMUNICACIONES, tanto fraudes de telefonía fija, móvil, televisión, injurias y calumnias que se cometen habitualmente.

■ REDES ABIERTAS, investiga sobre las novedades de las actividades delictivas y para la emisión de informes de actividades ilícitas como por ejemplo paginas que inducen a la anorexia.

La otra seccion SECCIÓN OPERATIVA se centra en tres actividades:

• Fraude en internet, donde irregularidades en redes ordenadores, informatica en general, el "grupo mixto" que se dedican a la investigacion de delitos informaticos, incluso la usurpacion de personalidad,

• Seguridad Lógica, seguridad en red, en informatica en general

• Propiedad Intelectual, se dedica a la investigacion de la piratería.

Y por último, la SECCIÓN TÉCNICA: que lleva a cabo labores de formación y estudios:

■ INFORMES APOYO TÉCNICO

■ FORMACIÓN Y ESTUDIOS I + D

Investigación de delitos que causan graves daños a la salud, como la venta de medicamentos contra la salud.

Estafas a través de las nuevas tecnologías

Si nos hacemos esta pregunta, ¿estafar por Internet? La respuesta sería se puede estafar a través de cualquier medio que facilita la red de redes: Páginas WEB, Correo electrónico, Portales de ventas/subastas, Servicios de mensajería instantánea, Mensajes a móviles y Otros: IRC, ICQ, Foros.…

Las Modalidades investigadas por el BIT son:

• Compra de productos y servicios con números de tarjetas válidos (CARDING). Donde para cometer un fraude no necesita de la tarjeta fisica, solo con los datos numéricos que circulan en la red es suficiente para cometer el fraude.

- Subastas y ventas ficticias, desde locutorios, por ejemplo.
- Transferencias Electrónicas Fraudulentas (TEF).
- Phishing.
- Pharming.
- Programas maliciosos.

Ejemplos de modalidades de fraude detectados por la BIT:

Subastas:

Con un locutorio, desde España se creaban paginas de subasta falsas, el dinero se derivaba a Italia y Rumanía a través de teléfono móvil. Un dato que habla de la globalización de este fenómeno es que a pesar de ser un delito cometido en territorio español no había usuarios afectados de nacionalidad española.

Phishing:

Se enviaba a los usuarios un correo suplantando la identidad de Adicae (Asociación de Ususarios de Bancos, Cajas de Ahorros y Seguros) para confirmar las claves de los bancos de los que eran clientes los receptores.

Comercios ficticios, donde venden cualquier tipo de producto. Ejemplo de de ello es la "Operación cargado", donde se detectó que se compraban productos a través de la creación de webs ficticias de recarga de movil, estas webs aparecian entre las primeras posiciones en los buscadores y nada mas que los usuarios entregaban los datos de sus tarjetas eran éstos utilizados fraudulentamente. Todo este tipo de webs eran creados por menores y se ponían en contacto entre ellos por redes privadas IRC.

Transferencias electrónicas fraudulentas por medio del famoso fraude conocido como "Cartas nigerianas". Infinidad de e-mails que utilizan la operativa del antigüo "timo de la estampita". Se envían correos masivos pidiendo el adelanto de un pago de un premio donde los autores son de origen Africano, de ahí su nombre.

Conclusiones y propuestas

■ Estos tipos de fraudes son ejecutados por organizaciones muy estructuradas y perfectamente organizadas, auténticas multinacionales del delito.

■ Utilizan escalones intermedios para la distribución, además de realizar el envío de rápido de dinero por circuitos de difícil y escaso control.

■ Estas organizaciones usan servidores ubicados en terceros paises, la mayoría de ellos sin ningún tipo de control y legislación que haga referencia a las nuevas tecnologías, la Sociedad de la Información y menos aún el fraude en medios de pago a través de internet.

■ Hay unas limitaciones territoriales y jurisdiccionales que obstaculizan las investigaciones que se llevan a cabo. Pero se utiliza muchisimo en las investigaciones la colaboración internacional. Por ello es necesario la colaboracion global en la lucha contra el fraude.

■ El robo de identidad es esencial en el delito economico, aunque todavia no hay un excesivo crecimiento con los datos que maneja la IT.

■ **D. Peter Gouwy**
Intelligence analyst(Europol)

¿Qué es Europol? Funciones e historia.

Europol es el cuerpo de seguridad de la Unión Europea, del que forman parte 27 Estados miembros de la UE más 14 que no son miembros de la UE y 10 organizaciones internacionales y se encarga de gestionar la información confidencial en el ámbito de la delincuencia. El objetivo de Europol es contribuir significativamente a la cooperación entre las autoridades competentes de los Estados miembros responsables de la prevención y la lucha contra la delincuencia organizada y el terrorismo internacional.

Europol fue instituido en virtud del Tratado de la Unión Europea de 7 de febrero de 1992. Con sede en La Haya, Países Bajos, Europol inició a sus operaciones el 3 de enero de 1994, denominándose 'Unidad de Drogas de Europol (UDE)' y con un mandato limitado a la lucha contra los delitos relacionados con los estupefacientes..

El Convenio Europol fue ratificado por todos los Estados miembros de la UE y entró en vigor el 1 de octubre de 1998. A instancia de diversos actos jurídicos relacionados con el Convenio, Europol se convirtió en organismo plenamente operativo el 1 de julio de 1999.

Progresivamente se añadieron a sus competencias otros ámbitos de la delincuencia. El 1 de enero de 2002 se amplió el mandato de Europol hasta abarcar todas las formas graves de delincuencia internacional, tal como se enuncian en el anexo al Convenio Europol. Desde 2007 se abarcan también los delitos de blanqueo de capitales.

Europol apoya las actividades policiales desarrolladas por los distintos Estados miembros, principalmente en los ámbitos de la lucha contra:

- El tráfico ilícito de estupefacientes.
- Las redes de inmigración clandestina.
- El terrorismo.
- La falsificación de moneda (euro) y de otros medios de pago.
- La trata de seres humanos (incluida la pornografía infantil).
- El tráfico ilegal de vehículos.
- El blanqueo de capitales.

Otros ámbitos prioritarios de la actividad de Europol son los delitos de violencia contra las personas, los delitos financieros y la ciberdelincuencia.

Europol entra en acción cuando hay implicación de una estructura delictiva organizada y se ven afectados dos o más Estados miembros.

Europol brinda apoyo a los Estados miembros:

Facilitando el intercambio de información, conforme a la legislación nacional, entre los funcionarios de enlace de Europol (FEE). Los FEE son destacados en comisión de servicio a Europol por los Estados miembros en tanto que representantes de sus cuerpos y fuerzas de seguridad;

■ Efectuando análisis operativos en apoyo a las operaciones;

■ Elaborando informes estratégicos (p. ej., evaluaciones de amenazas) y análisis de las actividades delictivas, sobre la base de la información y de los datos proporcionados por los Estados miembros y por terceros;

■ Poniendo a su disposición conocimientos especializados y asistencia técnica en las investigaciones y operaciones llevadas a cabo en la UE, bajo la supervisión y la responsabilidad jurídica de los Estados miembros correspondientes.

Europol también promueve activamente los análisis de actividades delictivas y la armonización de las técnicas de investigación en los Estados miembros. Europol tiene una colaboración internacional directa. La red de Europol apoya a 27 Estados miembros, a 14 Estados no miembros, la Unidad Europea colabora con 10 organizaciones internacionales.En aras de esta colaboración tiene dos tipos de Acuerdos: Operativos, donde intercambian datos personales y Estratégicos, donde no se intercambian datos personales.

Hay acuerdos operativos con Noruega, Suiza, Islandia, Croacia, Austria, Canadá y Estados Unidos. En la actualidad se está tratando de formalizar acuerdo operativo con Ucrania. Acuerdos estrategicos con Albania, Bosnia Herzegovina, Colombia, Macedonia, Moldavia, Rusia y Turquia.

El intercambio de información

La Europol tiene en todos los paises un oficial de enlace y una Unidad Nacional. Existiendo unos ficheros de trabajo analítico. La informacion es recibida, analizada y se envía a la Unidad Nacional de Europol. Con empresas privadas no se intercambia información y con Bancos, Visa, Mastercard, los datos personales no los reciben pues éstos pertenecen al Estado Miembro. Si se envía a la Europol está supervisada por el Estado.

El fraude en las tarjetas (skimming)

A nivel estrategico Europol ha redactado un informe sobre el problema global que existe en internet, de cómo funcionan el fenómeno del pharming o del phishing. En los casos de Carding, se formó a los paises miembros para la indicación de formas de actuar en estos casos.

A nivel operativo, Europol trabajó con el tipo de fraude denominado “skimming”, copia de tarjetas de banda magnética (Este año 2009, los delincuentes interceptaron 250 mil tarjetas que es casi la cantidad de tarjetas que se emitieron en España). Los cajeros automáticos y los TPVs pueden ser manipulados por los delincuentes. También se ha detectado “hacking” de las nuevas tarjetas con chip (Sistema EMV). Es mejor una tarjeta de banda magnética porque el chip, por ejemplo, no se utiliza en EEUU y éstos pueden ser copiados por 60 o 80€ por los delincuentes. Seguramente, con adelantos tecnológicos y logísticos dentro de un tiempo estos costes se abaratarán. Respecto al Carding, Europol informa y forma a la policia de los Estados miembros en este tipo de casos. Asi mismo también se mantienen reuniones con el sector privado (entidades financieras y junto Sistemas de Pago). Hay un equipo de seguridad que cubre en casi todos los paises europeos. Europl también ha mantenido reuniones con compañias de aerolineas porque ellas también sufren muchisimos fraudes con sus tarjetas.

Por último, decir que Europol colabora con Interpol y estan creando una web de colaboración en este tema del fraude en tarjetas.

Plan de recogida de datos y Ficheros de trabajo

¿De qué personas recopila la información Europol?

Los datos están referidos a las personas que sean "sospechosas", de acuerdo con cada derecho nacional, de haber cometido, o de haber participado en un delito, sin necesidad de haber sido condenadas por ello, y de las que se presuma que puedan cometer algún delito en el futuro.

¿Qué datos informatiza Europol?

Nombre, apellidos, alias, fecha y lugar de nacimiento, nacionalidad, sexo y "otras características útiles para la identificación", delitos, hechos imputados "o que puedan serlo", condenas y sospecha de pertenecer a una organización delictiva, así como cualquier "información complementaria”.Paralelamente, Europol ha creado lo que denomina “Ficheros de trabajo”, en los que almacena, modifica y utiliza datos referidos a las personas anteriormente mencionadas, a personas que sean consideradas "posibles testigos" en investigaciones, aunque ni siquiera haya una causa penal abierta, perjudicados, o respecto de las cuales haya "motivos para presumir que puedan ser perjudicadas" personas "intermediarias y acompañantes", así como personas "que puedan facilitar información" sobre delitos.

Una vez que se tiene toda la informacion se facilita a la Policía Nacional de los Estados miembros y ofrecen apoyo a éstos para poder acercarse a otros paises para compartir la informacion, pues los delincuentes no tienen fronteras.

■ **D. Alfonso de Miguel**
Capitán de la Guardia Civil (Grupo de Delitos Telemáticos)

El ciudadano contacta con la Guardia Civil: un sensor de la realidad del fraude

Existen dos direcciones de correo donde los ciudadanos pueden comunicar a la Guardia Civil los fraudes de los que han sido victimas. Estas dos direcciones de correo, funcionan como dos sensores que nos permiten sondear la informacion sobre la situación delictiva en nuestro pais.

Con la estadísticas realizadas a través de las comunicaciones a estas cuentas de correos, nos ha permitido llegar a la conclusion de con el paso del tiempo lo que varia es el modus operandi y que han descendido el número de comunicaciones de estos fraudes.

Análisis de las Estadísticas.

Analizando las estadisticas que tenemos en nuestro poder, en cuanto a "Estafas y Fraudes", hablando de cifras vemos que hay un 48% estafas B2C, un 5% de estafas C2B, un 16% de cartas nigerianas, un 13% de fraude en las telecomunicaciones, un 2% en carding, el 12% encuestas ficticias y el 4% de "Otros fraudes" (parejas,juegos online,..).

Podemos decir que existe una continuidad respecto del año 2008 y que las modalidades siguen siendo las mismas, pero con una distinta ejecución, lo que llamamos el "flash fraud"(fraude rápido).

Referente al Phishing, se ha notado que existe un descenso respecto a 2008 en cuanto a cantidad, y se ha producido un descenso en las comunicaciones por usurpación de paginas bancarias. La víctima que sufre un fraude de este tipo por regla general no va a realizar una denuncia. Por tanto las comunicaciones por usurpacion estan desapareciendo.

La mejora con el tiempo de la ciberdelincuencia es abismal, aunque no hay nuevos tipos de fraudes, las modalidades siguen siendo las mismas, pero con una distinta ejecución. Ahora se dedican al perfeccionamiento en la captacion de mulas con fórmulas mucho mas estudiadas, un email con oferta de trabajo, por ejemplo.

Como dato curioso podemos decir que el 80% de los equipos informaticos se encuentran afectados por virus y que un 40% de los ordenadores estan comprometidos por troyanos.

China es el mayor beneficiario del dinero de estafas electronicas, con usurpacion de indentidades. Hay una estafa del comprador, en la que un señor pone un bien en venta y el falso comprador le pide todos los datos posibles de la venta, una vez recopilados los datos , coge esos datos para ofrecer el mismo bien en otro pais. El fraude de parejas, donde se mandan 6 u 8 mensajes desde Costa Marfil con chicas espectaculares que pedian dinero para el peaje.

Por tanto,de las estadisiticas analizadas podemos concluir que han descendido las comunicaciones de phishing, pero se siguen cometiendo puesto que no ha descendido el número de casos phishing y que existe una especialización del agresor, con la automatizacion de la amenaza por medio del uso del malware bancario y un desconocimiento por parte del usuario de la amenaza malware.

Investigación y cooperación policial. Impedimentos de jurisdicción.

Se investigan las estafas, fraudes y phishings, pero en ocasiones se tropieza con la dificultad de identificar unos hechos con un mismo sospechoso. También se investigan los microfraudes por parte de rumanos en su mayoria, que recibian activos en la cuenta bancaria. Podemos decir que existe cooperacion internacional policial al ahora perseguir estos fraudes, sin embargo cuando para perseguir al delincuente se necesita una orden judicial, se topa con el Ministerio Judicial, y hay que procesar judicialmente al delincuente y si un juez no tiene jurisdiccion el procedimiento se complica.

Conclusiones y propuestas

En cantidades absolutas no se aprecia la incidencia de la crisis económica, si bien puede haber aumentado "la cifra negra" (casos que no se denuncian y de los que por tanto no se llega a tener constancia nunca) y se aprecia la variacion en el modus operandi, confimando el uso del malware tipo troyano en casos phishing.

Entre las muchas de las medidas para minimizar los efectos del fraude en medios de pago propongo las siguientes:

■ Sistemas de confirmación de movimientos Web (SMS´s o call center). Así, cada movimiento que se produzca en la cuenta del usuario es comunicado a éste en tiempo real, con lo que éste ante una operación no realizada bajo su consentimiento podrá actuar para tomar las medidas necesarias y evitar así un mayores daños en su cuenta (cancelación de la cuenta bancaria meidante aviso a la entidad financiera y denuncia policial).

■ Bloqueo preventivo de cuentas. En ocasiones, las entidades tienen conocimiento de actividades fraudulentas y la cuenta no se bloquea, exige una denuncia, pero muchas veces esa denuncia no se produce por miedo. Hay gente que está en contra de estos bloqueos preventivos de cuentas por el temor de no poder realizar operaciones, pero es preferible un bloqueo preventivo que luego lamentar el saqueo de todo el dinero que se encontraba en la cuenta.

■ **D. Diego Alejandro**

Inspector del Grupo 1, de Medios de Pago de la Comisaría General de la Policía Judicial del Cuerpo Nacional de Policía de España.

¿Qué es una organización criminal?

Son aquellas que tengan por objeto cometer algún delito o, promuevan su comisión, así como las que tengan por objeto cometer o promover la comisión de faltas de forma organizada, coordinada y reiterada. Los criterios que destacan de estas organizaciones son:

1.- Colaboración de dos o más personas.
2.- Reparto de tareas específicas
3.- Permanencia en el tiempo. (6 meses)
4.- Mecanismos de control o disciplina interna.
5.- Sospecha de comisión de delitos graves.
6.- Actividad Internacional.
7.- Empleo de violencia o intimidación.
8.- Empleo de estructuras comerciales o económicas.
9.- Implicaciones en blanqueo de capitales.
10.- Influencias políticas, medios de comunicación, etc.
11.- Búsqueda de beneficios o poder.

Es necesario mencionar también que estas bandas organizadas están jerarquizadas y tienen sus funciones muy bien delimitadas y definidas. En cuanto a los AGENTES intervinientes en el fraude, tenemos que hacer mención al Proveedor, Falsificador, Pasador, Receptador. Tambien tenemos la figura del Colaborador que abarca a "connivente", "mulas", Contravigilancia, blanqueador, testaferro, etc.

MODALIDADES DELICTIVAS:

■ Tarjetas robadas / extraviadas: Tarjetas "calientes".

■Tarjetas no recibidas por el titular.

■ Solicitudes falsas de tarjetas de crédito para conseguir soporte fisico y obtener el numero PIN.

■ Utilización fraudulentas de numeraciones (CNP).

■ Falsificación de Tarjetas:

- Falsificación electrónica
- "Plásticos" Blancos, se venden por internet y se utiliza para materializar el fraude.
- Alteración de la personalización
- Falsificación Íntegra

Problemas de la investigacion

El ámbito territorial de este fenómeno es de carácter internacional. Pues las tarjetas bancarias, pueden ser de origen español y ser usadas tanto en España como en el extranjero, y por otro lado las tarjetas pueden ser extranjeras y usadas en España.

Otro dato a tener en cuenta es que se tratan de Redes Internacionales de gran movilidad, que existe un aumento de la Especialización y Organización de los Grupos Criminales, que cambian de Teléfonos y como Medida de Seguridad debería haber una Reacción Judicial, pues ésta es tardía.

Otro porblema es que una colocación de dispositivos las realizan en fines de semanas, puentes y festivos y en otras ocasiones el tiempo trascurrido entre la clonación y la detección del fraude es bastante elvado. Se denota la falta de colaboración de los establecimientos, en cuanto a la facilitacion de la grabaciones y reconocimientos, y tambien la falta colaboración de Entidades Financieras pues hay una lentitud en las respuestas, informaciones incompletas o inexistentes.

Obstaculos para la persecución del delincuente

Es flagrante la falta de medidas preventivas en algunas entidades financieras: la ausencia de cámaras de seguridad (que graben), que las grabaciones sean de poca calidad, falta de revisión periódica de cajeros e instalación de sistemas técnicos de detección de dispositivos, etc. En lo que concierne a movimientos fraudulentos en el extranjero el Cuerpo Nacional de Policía se encuentra con la inexactitud de la información y la falta de colaboración judicial y policial con otros países. A estos problemas hay que añadir la faci-

lidad del uso de Internet, lo cual supone el favorecimiento del anonimato, conexiones a redes inalámbricas y conexiones en cibercafés o locutorios.

Financiación de delitos e internacionalización.

Es característico que detrás de la comisión de estos delitos se escondan organizaciones delictivas que utilizan este dinero defraudado para la financiación de otro tipo de delitos: falsificación de documentación, matrículas, robo y venta de vehículos de alta gama, droga (distribución y cultivo), armas, etc. ES normal pues, que estas organizaciones no solo se dediquen al fraude en medios de pago, sino que diversifican "su negocio". Además, también en característico que sean internacionales, tanto por la composición de sus miembros como por los lugares donde operan y/o cometen las diversas actividades delictivas.

Conclusiones y propuestas

Es necesaria e imperiosa la colaboración delictiva entre los diferentes grupos policiales, dentro de un mismo país, puesto que queda constatado la gran heterogeniedad de actos delictivos que pueden cometer estos grupos. A su vez, también es necesaria la colaboración entre diferentes Cuerpos policiales de diferente países, a la vez que Europol e Interpol deben coordinar la gestión de toda la información facilitada por estos cuerpos policiales.

Pero aunque esta colaboración fuese totalmente efectiva se quedaría en nada sin la labor de los jueces y la administración de justicia de los países involucrados. Tras una labor de investigación es necesaria la colaboración y actuación de jueces que a su vez, tengan capacidad de poder juzgar con normativa acorde a los tiempos en los que estamos. Muchos casos investigados y detectados se quedan sin ser juzgados o ser perseguidos por la justicia debido a que estos jueces por la normativa existente no son competentes para entrar a conocer estos hechos.

LA DELIMITACIÓN DE LA RESPONSABILIDAD EN EL FRAUDE, LA GRAN ASIGNATURA PENDIENTE PARA LA CONFIANZA DE LOS USUARIOS

■ **D. Alejandro Salcedo**
Coordinador del Instituto de Consumo de Castilla La Mancha

Progresión del fraude en la Sociedad de la Información

En un entorno en el que cada vez más se utilizan los diferentes medios de pago para realizar cualquier tipo de compra, también las habituales, es necesarioque se garanticen la seguridad de los medios de pago. Es evidente la progresión del fraude en el marco de la Sociedad de la Información, donde las nuevas tecnologías cada vez están más presentes en nuestras vidas. Esto fomenta el aumento del fraude, pero además que éste no sea homogéneo y que se propague con mucha facilidad y rapidez, utilizando uno de los pilares de la Sociedad de la Información: Internet.

A parte de estas característias dominantes en todos los tipos de fraude que están sufriendo en la actualidad los consumidores, hay que sumar una situación coyuntural de crisis económica que hace que los delincuentes aprovechen posibles situaciones de debilidad en las que se encuentran los consumidores (por ser comunes a muchos de ellos) para cometer un fraude: ofertas de empleo, juego, lotería y apuestas, filantropía, etc).

La normativa existente

En este escenario es necesario mencionar qué normativa regula esas situaciones de fraude. La primera a la que quiero hacer referencia es la Recomendación de la Comisión europea de 1988 en la que la Asociación Europea de Bancos y de Cajas de Ahorros aceptaron cumplir en 1.990. En ella la responsabilidad del titular de tarjeta por utilización fraudulenta tras robo de tarjeta, quedó fijada en 150 euros: límite máximo de responsabilidad del consumidor hasta el momento de la notificación del robo o perdida de la tarjeta. En la mayoría de falsificaciones, así como en los casos de robo y extravío se debe restituir en 24, 48 ó 72 h.

Papel de las administraciones

Al igual que otros muchos actores, es necesario un papel activo por parte de las administraciones publicas en materia de consumo. Pero para una correcta actividad que vaya encaminada a la erradicación del fraude es necesario destacar varias ideas presentes en la actualidad:

- Hoy en día las funciones que tiene la administración de consumo son limitadas (tramitación y mediación). A eso se suma que en una transacción comercial en la que pueda cometerse un fraude en medios de pago pueden intervenir varias administraciones, e incluso varias áreas dentro de una misma administración, a parte de los Cuerpos y Fuerzas de Seguridad del Estado. Por lo que pueden concurrir varias competencias administrativas y éstas pueden entrar en conflicto.

- Son evidentes las limitaciones de los recursos públicos. Las técnicas, los fraudes van muy por delante de las Administraciones Públicas. Los costes de actuación de este tipo control previo al fraude implica gastos.

Debemos tener en consideración 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. 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. El objeto de la presente ley es incorporarla al ordenamiento jurídico español. La presente ley entrará en vigor el 1 de noviembre de 2.009. Esta ley refrenda la práctica habitual en la banca.

– Los mecanismos de resolución en materia de consumo son insuficientes. Además es evidente la ausencia de normas, y la dificultad para resarcir al consumidor, puesto que es muy difícil encontrar al delincuente y las entidades financieras no asumen responsabilidad alguna.

– Ausencia de vías de coordinación y concertación.

– Desajuste de las expectativas ciudadanas. Es palpable el descontento de los ciudadanos con su situación actual en lo que concierne al fraude en medios de pago.

– En la actualidad, este tema, el fraude en medios de pago, aparace como una actividad contingente en la agenda pública de consumo, a pesar de su magnitud.

Propuestas de actuación

Vistas las carencias existentes en este tema es necesario abordar este problema tomando como prioritarias varias soluciones simultáneas:

Asunción de la corresponsabilidad, cubrir los vacíos normativos.

Políticas preventivas:

- Necesidad de Estudios de diagnostico de la situación.
- Control programado:
  - Protocolos de seguridad en la red.
  - Rastreo de páginas web.
  - Análisis documental
  - Mistery Shopping
  - Red de alerta de seguridad electrónica (debe de ir acompañada de acciones de cesación)
  - Medidas de carácter disuasorio (ficheros; publicidad; sanciones; …).

– Políticas de protección.

• Establecimiento de mecanismos de resolución y resarcimiento “ad hoc” (modalidad arbitral; fiscalía de consumo; sistemas de garantías; …).

• Coordinación inter e intra-administrativa.

• Acción concertada.

– Políticas de promoción.

• Facilitación de recursos.

• Información y divulgación.

• Campañas de sensibilización y difusión.

• Formación en destrezas para el manejo electrónico.

• Programas de educación financiera.

• Estrategias de discriminación positiva (distintivos, acreditaciones, promociones, etc.).

• Especial atención a los colectivos vulnerables (discapacitados, personas mayores, inmigrantes, escasos recursos económicos, nivel cultural bajo, “analfabetismo digital”, …).

■ **D. D.Pablo Mayor**
Abogado del equipo jurídico de ADICAE

El examen de la responsabilidad en el fraude y su posterior delimitación presupone:

■ La existencia de una situación en la que cualquier participante en el tráfico jurídico o mercantil (nos centraremos en los consumidores o usuarios) haya resultado perjudicado.

■ La existencia de una acción dirigida contra el PATRIMONIO del consumidor [que ve sus intereses truncados de alguna manera].

■ La necesidad de comparar los intereses en juego al fin de determinar que operador debe responder, que operador ha sido imprudente o ha incurrido en mala practica.

■ Como conclusión vemos que la determinación de la responsabilidad en el fraude es una operación eminentemente lógica y en la mayoría de las ocasiones judicial.

Sobre esta base nos podemos formular dos preguntas:

1º.- Quien asume responsabilidad ante una situación de fraude en el ámbito financiero.

2º.- ¿El consumidor es siempre el responsable?

Esta es la percepción que se tiene normalmente, es una visión un poco PESIMISTA, y muy poco realista de la situación.

Podemos partir de un supuesto real: En la Asociación nos hemos encontrado con el caso de una persona que le pasan distintos cargos a la tarjeta. Investigando el origen de los cargos sospechamos que se puede deber a la existencia de correo de las entidades que consigna todo el numero de cuenta, lo que unido al DNI y a una dirección lleva a que se le pasen cargos. Evidentemente y sin necesidad de mayor análisis podemos inferir que la conducta de la entidad financiera no es diligente pues permite el conocimiento del número de cuenta por terceros ignorando unas medidas de seguridad mínimas.

Como punto de partida de estas reflexiones diremos que por todos son conocidos los riesgos que entrañan tanto la CONTRATACIÓN A DISTANCIA (Ej. la compra por catalogo) como la contratación por VIA ELECTRONICA -como una de las especialidades de contratación a distancia-.

En particular podemos afirmar que es muy controvertida la seguridad de las tarjetas de crédito -como medio de pago masivamente utilizado y que entraña evidentes peligros de uso fraudulento-, y en concreto por ejemplo actividades de clonación, sustracción del pin, etc. En general es muy controvertido el sistema de seguridad de los instrumentos de pago pues en el tráfico jurídico se contraponen los principios de seguridad y rentabilidad económica (mayor seguridad del sistema exige mayor inversión y resta rentabilidad).

Ello hace que nos encontremos con fenómenos como:

- "Phishing", que consiste en obtener las claves de los usuarios a través de mensajes falsos (sistema activo del defraudador).
- "Pharming", donde se altera la barra de direcciones del navegador de usuario, provocando que cuando este acceda a un banco o tienda "on line" aparezca en su lugar un página falsa (sistema pasivo del defraudador).
- Clonación y duplicado de tarjetas que supone aproximadamente el 10% del fraude realizado con tarjetas.
- Sustracción de la tarjeta (por el método tradicional o por medio del archiconocido lazo libanes).
- Apropiación de claves en el comercio electrónico y en la banca por Internet.
- Otros.

Evidentemente es un sistema que se publicita como seguro por las entidades y todos sabemos que no lo es al cien por cien.

Como ejemplo del tratamiento de la jurisprudencia podemos citar la Sentencia núm. 101/2004 de 23 noviembre de la Audiencia Provincial de Islas Baleares (Sección 1ª) que señaló: *"Y de dicha operativa mendaz se concluye linealmente que existe un engañado, el Banco o Caja, que ha proveído al acusado de la T.P.V., (...); y existe un perjudicado, que no es el titular de la tarjeta, pues cuando éste rechaza el cargo y la central de tarjeta reclama al Banco o Caja que facilita la T.P.V. que a su vez recabe los justificantes firmados por el titular de la tarjeta, cuando el Banco o Caja se da cuenta del engaño de que ha sido víctima no puede, lógicamente, facilitar justificantes cuando no ha habido operaciones, por lo que tiene que retroceder a la central de tarjetas el importe abonado por ésta, soportando la pérdida del dinero que el sujeto activo ha extraído, antes de ser descubierto el operativo".*

Este ejemplo nos sirve como punto de partida del hecho que fundamenta la atribución de responsabilidad: al no ser

seguro al 100% el sistema se opera sobre la presunción de que las entidades al igual que soportan los beneficios de la operativa electrónica (facilidad y promoción de su uso) deben soportar los perjuicios y quebrantos que se ocasionen por tal motivo. Si bien normalmente se sigue este criterio entre los Jueces y Magistrados el criterio económico dificulta el acceso a la justicia de los particulares en el sentido de desincentivar la eventual demanda a la entidad financiera por el simple hecho de que el particular debe soportar el gasto derivado del acceso a la Justicia, lo cual en determinadas ocasiones es muy gravoso (pues supone que además de soportar un daño a su patrimonio el particular deba realizar una "inversión" para intentar recuperarlo).

Desde las Asociaciones, y en particular desde ADICAE venimos aplicando, tras las gestiones extrajudiciales necesarias, el principio de "poner la denuncia, poner la demanda": cuando se tiene conocimiento de un presunto hecho delictivo debe ponerse la denuncia (de hecho en muchas ocasiones hechos delictivos evitan los mecanismos de detección por el hecho de que debido a las escasas cuantías del fraude no son siquiera denunciados); por el contrario la entidad utilizará este hecho para señalar que el perjudicado no ha intentado perseguir al supuesto culpable, intentando eximirse de la responsabilidad civil derivada del delito.

Sin perjuicio de lo anterior, la existencia de fraude ha determinado que se establezcan sistemas de seguridad preventivos y reparadores.

■ Los preventivos son aquellos protocolos que establecen las entidades para evitar el fraude. Sirva decir que como ejemplo de medio preventivo al fraude en otros países (Reino Unido y Francia sin ir más lejos) se utiliza habitualmente un sistema de cobro con **APARATOS TPV MOVILES** en los que se introduce la tarjeta y el usuario marca (secretamente) el pin en el lugar de situación del cliente mientras que en España se llevan nuestra tarjeta. Este sistema se ha visto idóneo para evitar las situaciones, cada vez más frecuentes, de clonación.

■ Los reparadores, por el contrario, son aquellos que se despliegan por el ordenamiento jurídico para "compensar" y restaurar una situación de fraude. En este punto nos encontramos con el problema de la excesiva judicialización, como principal escollo con el que se enfrentan los consumidores (haciéndose necesaria la instauración de sistemas extrajudiciales de reparación, más rápidos y con menor coste).

En este orden de cosas, y en el ámbito concreto de la contratación electrónica, podemos señalar que el pago mediante tarjeta en las ventas a distancia genera siempre cierta desconfianza. El hecho de que el consumidor titular de la tarjeta tenga que comunicar su PIN a través de internet provoca cierto recelo ante la **POSIBLE CAPTACIÓN** de esos datos por terceros, los cuales podrían utilizar aquéllos para la realización de actos fraudulentos, e incluso sin ser identificados.

Como reflexión podemos pensar en cuantas veces hemos visto el aviso que dice que estamos operando con una conexión segura y cuantos casos conocemos de fraude. Es claro que el problema básico en estos supuestos (ventas a distancia electrónicas) es la ausencia física simultánea de los contratantes que impide la identificación tanto del titular de la tarjeta de pago como de la tarjeta misma, abriendo un vasto terreno a los que pretende servirse del sistema para cometer el fraude. Todo ello unido a que tampoco se obtiene un comprobante de la venta firmado por el titular de la tarjeta determina que nos encontremos como ventaja e inconveniente simultaneo el anonimato, y la abstracción de los medios de seguridad.

En este punto conviene señalar que desde la experiencia de las asociaciones de consumidores, y en particular de ADICAE nos encontramos con que **A LAS PROPIAS ENTIDADES NO LES INTERESA UN SISTEMA DE SEGURIDAD COMPLEJO (Y POR ELLO MÁS SEGURO) QUE DESINCENTIVE SU USO POR LOS CONSUMIDORES**, habiéndose descartado diversos sistemas y proyectos bien por motivos de coste (identificación de huellas dactilares, iris, etc.) bien por motivos de excesiva complejidad.

Como todos conocemos, en la práctica de esta operativa, el empresario se limita a pedir al consumidor el número de tarjeta y la fecha de caducidad de ésta, y en el mejor de los casos las tres cifras del código de seguridad para transacciones internacionales de la parte de atrás. No obstante en la actualidad, es habitual que se exija el tecleo, junto con el número de la tarjeta, de un pin o número secreto al ejecutar la orden de pago, lo que permite garantizar, en mayor medida, la seguridad de la transacción. Es decir, a priori, el fraude exige el conocimiento de 19 dígitos y la fecha de la caducidad de la tarjeta. **A PRIORI NO PARECE DIFICIL**, dada la expansión del conocido "malware" destinado a obtener los datos de los usuarios y los "troyanos" que se instalan en nuestros ordenadores.

En particular en lo relativo a las tarjetas nuestro legislador protege a los titulares de aquellas frente a la utilización indebida o fraudulenta del número de ésta en las ventas a distancia, dando **RELEVANCIA PENAL**. En el ámbito penal, el art. 248.2 del Código Penal tipifica el delito de fraude informático, y considera "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". Evidentemente este supuesto está pensado, entre otros, para la duplicación de tarjetas.

Por otro lado en el ámbito civil, el art. 106 del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios regula el pago mediante tarjeta, siendo su lectura necesaria para comprender la protección que el legislador otorga a los consumidores y usuarios. De la lectura del citado artículo podemos inferir que el titular de la tarjeta cuyo número ha sido utilizado indebida o fraudulentamente por un tercero tiene **DERECHO A ANULAR EL CARGO** por la entidad de crédito, debiéndose efectuar, en un plazo no superior a treinta días desde la comunicación de

la solicitud de anulación, las respectivas. Esta posibilidad otorga al consumidor la seguridad de que podrá rechazar las disposiciones mientras los hechos en los que se ha producido se investigan penalmente. Además, conforme a la jurisprudencia antes revisada, es el empresario quien tendrá que probar que el número de la tarjeta utilizada para pagar esas compras electrónicas a distancia ha sido introducido por el titular legítimo. En este sentido se produce una inversión de la carga de la prueba en beneficio del consumidor, lo que supone un refuerzo vital para la seguridad del tráfico en Internet, máxime a la vista de la creciente popularización de todos estos sistemas. Por otro lado el banco emisor de la tarjeta sólo es responsable de la utilización indebida o fraudulenta del número de la tarjeta de pago si incumple el contrato de emisión suscrito con el titular, como vimos en el supuesto de inicio. Además de lo señalado, resulta evidente que la actuación negligente del titular de la tarjeta de pago le hace responsable frente al empresario y frente al banco emisor, de los daños y perjuicios ocasionados (por ejemplo, por haber comunicado a un tercero el número de la tarjeta o por no haber puesto en conocimiento del banco emisor de la tarjeta su extravío o sustracción), correspondiéndole al titular de la tarjeta la carga de la prueba. *EJ: PIN APUNTADO EN LA PARTE DE ATRÁS DE LA TARJETA.*

A la vista de lo señalado podemos concluir que se puede solicitar la anulación de aquellos cargos que se consideren fraudulentos, y que ante dicha solicitud de anulación del cargo por parte del titular de la tarjeta, en relación a ese uso indebido o fraudulento del número de la tarjeta en una venta realizada por Internet, el empresario soporta el riesgo de la operación comercial, sin que pueda entrar a valorar si, efectivamente, el número de la tarjeta se ha utilizado correctamente por su titular o indebida o fraudulentamente por un tercero. De este modo, el titular de la tarjeta recibe protección, si no se ha hecho efectivo el daño.

En otro caso y sí si se han hecho disposiciones de cantidad **REITERAMOS QUE LA PROTECCION SE OBTIENE ÚNICA Y EXCLUSIVAMENTE POR VÍA JUDICIAL**, puesto que tanto los Servicios de Defensa al Cliente de las entidades como los servicios de reclamaciones del Banco de España y de la CNMV no indican nunca en sus informes referencia a los daños y perjuicios causados al consumidor, que son fijados por los Tribunales, con la excepción, por supuesto, de aquellos casos en los que las entidades extrajudicialmente ofrecen por este concepto cantidades para evitar tener que llegar al procedimiento.

Podemos señalar que hemos comprobado que ante la especialidad de muchos contratos y la concreción de aspectos de consumo prevalecen los dictámenes técnicos de los Órganos Supervisores, por lo que es fundamental el **ASESORAMIENTO EXTRAJUDICIAL** sobre todo en la formulación de las reclamaciones que irán a los supervisores para poner las bases del reconocimiento judicial de la responsabilidad.

Volviendo a las referencias a los sistemas de seguridad se debe señalar que en las transacciones el emisor de la tarjeta entrega al titular un número de identificación personal y secreto (NIP o PIN en lengua inglesa), el cual añade mayor seguridad en la adquisición de los bienes y servicios on line. En las ventas electrónicas, la introducción del **NIP (Y AHORA LA UTILIZACIÓN DE LA TARJETA DE CLAVES –CUADRICULA QUE ENTREGAN ALGUNOS BANCOS COMO SISTEMA AÑADIDO DE SEGURIDAD-)** supone la identificación del titular, que es necesaria para que el sistema de pago electrónico funcione correctamente. Con el NIP, el banco acepta la venta electrónica si el titular de esa clave tiene fondos y la tarjeta sigue en vigor. Estos sistemas, el PIN o NIP, en primer término y la cuadrícula de claves, que se está popularizando como medio de evitar el "malware" que copia y retiene las teclas que se presionan suponen un medio y un modo de evitar la responsabilidad por las entidades de crédito. En este punto nada diremos por cuanto la mayor seguridad del sistema redundadará siempre tanto en beneficio del propio consumidor como de la propia entidad que no tendrá que soportar quebrantos sólo por la falta de prueba.

EN ESTE SENTIDO LA PRUEBA DE LA NEGLIGENCIA EN LA UTILIZACIÓN DEL PIN O LA FALTA DE CUSTODIA DE LA TARJETA PUEDEN EXONERAR A LAS ENTIDADES DE CREDITO DE RESPONDER. *EJ, si le entrego la tarjeta a un tercero o alguna situación similar.*

De hecho es el argumento que normalmente utilizan para justificar la no respuesta a las pretensiones del consumidor.

Podemos citar otro caso con el que nos hemos encontrado en la Asociación, el de un padre con dos hijos que tienen abiertas cuentas de ahorro vivienda en un banco. Se produce la transferencia inconsentida a un tercero de las cantidades de la hija y no se consigue retrotraer. Después se produce la del hijo y si se consigue parar. La entidad manifestó que hubo una mala utilización del PIN de banca electrónica del padre para eludir su responsabilidad. En el supuesto comentado hubo que pasar por la correspondiente reclamación al defensor del cliente, al Banco de España, y posteriormente el juicio. Finalmente se negoció "en la puerta del Juzgado" la devolución del dinero, tres años y medio después.

En este supuesto nos encontramos con problema de no llegar a la transacción: que el banco recurra y que se tarden otros tres o cuatro años mínimo en conseguir la devolución del dinero (sin perjuicio de la eventual ejecución provisional que, de nuevo, encarecería, el proceso). Evidentemente esta actuación es conforme al Derecho pero no es ética en los términos en los que se plantea la responsabilidad social corporativa, tan fervientemente defendida por las entidades de crédito.

En este orden de cosas, aún en el caso de que el titular hubiese actuado negligentemente, comunicado a un tercero el NIP, o no habiendo puesto en conocimiento del emisor de la tarjeta su extravío o sustracción, podría aquél anular el cargo, aunque posteriormente el empresario y el emisor de la tarjeta puedan reclamarle los daños y perjuicios ocasionados con su conducta .

Podemos citar un caso práctico resuelto en una sentencia de Abril de 2006, dictada por la Audiencia Provincial de las Islas Baleares, en el que un consumidor titular de una tarjeta solicitó a su Banco que le reabonara en su cuenta un cargo que no reconocía, realizado a través de una tarjeta de crédito emitida por dicho Banco pero que el consumidor negaba haber recibido. El Banco negaba ese reabono porque decía que sí había enviado la tarjeta, pero no lo probaba.

Evidentemente ante la falta de prueba el consumidor vio satisfechas sus pretensiones. En relación a la operativa de las tarjetas de crédito es obligado citar la Decisión Marco JAI/413/2001, de 28 mayo, del Consejo de la UE, relativo a la Lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, en cuyo artículo 1.a) se señala la definición de instrumentos de pago. Vid. Artículos 1 y ss. por lo sintético de las definiciones.

Es muy interesante para completar el concepto revisar la Consulta 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago y 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 multiviaje de los transportes públicos urbanos.

En relación a la normativa relativa a las tarjetas en España, podemos decir que se fundamentan como todos los contratos atípicos en la libertad contractual que consagra y reconoce los artículos 1.091 y 1.255 del Código Civil, no existiendo legislación positiva sobre las tarjetas de crédito, ni siquiera disposiciones de carácter fiscal o administrativo.

Como principal problema ante la falta de regulación nos encontramos con el de caso de robo o extravío, ya que en las condiciones pactadas se establece la obligación del titular-usuario de comunicarlo al emisor, dentro de ciertos plazos: telefónicamente, por escrito con un máximo de tres días, etc…

EN RELACIÓN A LA EXISTENCIA DE FRAUDE

El problema que surge en este punto es quien debe responder de la pérdida en el caso de existencia de una factura con firma falsificada. Según la Recomendación de la CE de 17 de noviembre de 1988, hasta el momento de la comunicación la responsabilidad del titular de la tarjeta queda limitada a 150€.

Esta Recomendación, a pesar de no ser vinculante, ha sido recogida por la gran mayoría de las entidades de crédito de nuestro país. Es, pues, habitual que el contrato de tarjeta de crédito celebrado con la entidad contemple que antes de la notificación el titular responda hasta una cantidad determinada, excepto en el supuesto de que haya actuado fraudulentamente o con negligencia grave. En cualquier caso, después de la comunicación, la responsabilidad es íntegramente de la entidad bancaria. En cualquier caso **HABRA QUE ESTAR A LOS LIMITES DE DISPOSICIÓN QUE SE ESTABLECEN COMO MEDIDA DE SEGURIDAD ADICIONAL.**

Uno de los problemas con los que nos encontramos en este punto, reiterando lo anteriormente mencionado, es que por las cuantías podemos definir estos supuestos como "microfraudes" lo que determina la dificultad de perseguir conductas como éstas.

Conclusiones y propuestas

A la vista de todo lo expuesto podemos concluir que si bien los sistemas de comercio electrónico y banca por Internet son relativamente seguros (no son seguros al 100%) y el consumidor está razonablemente protegido ante los fraudes y los ataques a su patrimonio, queda un largo camino para hacer "confiable" al 100% el marco de operaciones a través de internet. Como medida de choque a proponer para mejorar el sistema y la restitución de los derechos de los usuarios en aquellos casos en que sus legítimos intereses se hayan visto truncados, las asociaciones y Adicae abogamos por el establecimiento de sistemas extrajudiciales de resolución de estos conflictos, que permitan el acceso a la Justicia de todos los consumidores y usuarios sin coste, sobre todo a la vista de que en la mayor parte de las ocasiones debido a la existencia de los conocidos como "microfraudes" los criterios de viabilidad económica se anteponen a los de la Justicia material, evitando que muchas actuaciones sean perseguidas, determinando en último caso que permanezcan invisibles a las autoridades, con el especial peligro de que se perpetúen en el tiempo.

En España el legislador con artículos como el 106 del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios que regula el pago mediante tarjeta, y con el sistema de defensa de los usuarios unido al principio de inversión de la carga de la prueba, y los Jueces y Tribunales con una ascendiente sensibilidad por el Derecho del Consumo que se ve plasmada en la jurisprudencia, tutelan razonablemente bien los derechos de los consumidores.

No obstante lo anterior el papel de las Asociaciones, entre las que se encuentra Adicae como pionera del tratamiento de los supuestos en los que se produce un fraude a los usuarios financieros, se configura cada vez como más necesario, sobre todo a la vista de que el movimiento consumerista se fundamenta sobre la información y formación, cada vez más especializada y concreta, de los consumidores como medio para evitar estas situaciones y sobre el asociacionismo como medio de defensa, colectivo, de aquellos fraudes que afectan a cientos o miles de perjudicados.

IMPACTO DE LA CRISIS ECONÓMICA Y EL FRAUDE EN LOS PAGOS ON-LINE Y EL COMERCIO ELECTRÓNICO

■ **Dña. Elena García Díez**

Coordinadora de e-Fraude del Instituto Nacional de Tecnologías de la Comunicación (INTECO)

Desarrollo de la Sociedad de la Información

Para entrar a valorar el impacto de la crisis económica en el fraude on-line y el comercio electrónico es necesario primero centrar-se en la evolución y desarrollo de la propia sociedad de la información. La utilización de medios pago electrónicos registran una tendencia claramente al alza, a medida que también crece el nivel de desarrollo del comercio electrónico y sus diferentes medios de pago. El número de internautas o de consumidores que navega y utiliza internet para realizar sus compras cada vez es más elevado, y existe una diversificación cada vez más grande en su uso y en el tipo de compras que se realizan. Más allá de que la disponibilidad de algunos servicios esté lejos de considerarse óptima, llama la atención la tendencia a desarrollar más los servicios dirigidos a los ciudadanos que a las empresas (24 millones de internautas y 7,6 millones de hogares conectados en España) y la mayor atención prestada a los conceptos ligados a la generación de ingresos.

Día a día, Internet se está incorporando a un mayor número de actividades laborales, profesionales, personales y de ocio de los consumidores españoles. El 41% de los hogares ya cuenta con una conexión de Internet en España. Inicialmente, los consumidores utilizaban Internet para tareas sencillas, principalmente para comunicarse entre ellos y para buscar información. Sin embargo, y pese a que estas actividades siguen registrando un nivel muy alto de actividad, poco a poco los consumidores van realizando tareas más complejas y más trascendentes para su vida cotidiana. Así, es cada vez más frecuente observar como se planifican y contratan viajes, se busca empleo o se accede a una formación on-line para encontrarlo, se adquieren todo tipo de productos o se realizan operaciones bancarias como contratar una hipoteca.

Cabe destacar, sin embargo, que la disponibilidad o diversificación de una tecnología como Internet no implica automáticamente su uso. El acceso a Internet es condición necesaria, pero no suficiente para el desarrollo de la Sociedad de la Información.

Cultura de Seguridad del Usuario y uso de soluciones de seguridad en los hogares

Las incidencias relacionadas con la seguridad y la confianza de los usuarios en la Red son un factor crítico que condiciona el desarrollo de la Sociedad de la Información en España, retrasando la adopción y extensión de servicios a través de Internet, como el comercio electrónico, la administración electrónica o la banca on-line.

En relación con la seguridad de la información, los usuarios de Internet utilizan principalmente medidas de seguridad que no exigen ninguna participación activa (automatizadas), existiendo un déficit en la incorporación de medidas que reclaman mayor proactividad por parte del usuario.

Entre estas herramientas, los programas antivirus son la más generalizadas. Entre las razones para no implementar medidas de seguridad, las más importantes son las derivadas del desconocimiento o de la percepción de que es innecesaria. Es destacable el hecho de que un gran porcentaje de los usuarios que no utilizan programas antivirus alegan no hacerlo porque este entorpece el uso del ordenador y la navegación por Internet. En cuanto al efecto de las incidencias en los usuarios, las consecuencias más habituales son la actualización, renovación e instalación de nuevas barrera de proyección (el 10% instaló su primer antivirus, el 20% cambia de antivirus), el cambio de opinión y comportamiento respecto a la seguridad, siendo más prudentes, y reclamando mayor implicación de la administración. Un dato importante en este punto, es que las incidencias apenas modifican el uso de los servicios, debido al carácter de imprescindible que Internet está adquiriendo.

Aunque casi la mitad de los hogares indican que utilizarían más servicios si supieran reducir su riesgo, el análisis señala que, en general, las incidencias de seguridad no provocan que los usuarios abandonen servicios o dejen de utilizar Internet. Si bien es cierto que existe un efecto de retraso en la incorporación a la Sociedad de la Información relacionado con la falta de confianza en Internet, dicho efecto debe buscarse entre los "no usuarios", es decir, aquellos que no se sienten suficientemente protegidos como para incorporarse y moverse plenamente en la Red.

Así las cosas, los usuarios habituales de Internet han englobado de tal forma los servicios on-line en su estilo de vida que se les hace muy difícil prescindir de los mismos. En este contexto, las incidencias sufridas se interpretan como avisos para aumentar su equipamiento de protección y/o para mostrarse más prudentes en sus hábitos, pero no se interpretan como avisos de que deben abandonar o reducir el uso de Internet. Simplemente, para muchos usuarios, la segunda alternativa no parece posible.

A pesar de las incidencias declaradas, y del escaso conocimiento del riesgo que manifiestan los usuarios, la sensación general es de confortable seguridad en el uso de Internet. La gran mayoría considera que su conexión y su equipo les garantizan una navegación segura, cuando en realidad no suele ser así.

ndicadores de incidentes de fraude electrónico

Entre los muchos indicadores para localizar incidentes de fraude electrónico podemos contar, en primer lugar, con los Informes del Anti-Fraud Command Center de RSA o los del AntiPhishing Working Group. Estos informes, sin embargo, no recogen la globalidad de los datos a nivel técnico. En ellos, encontramos un ranking de países hacia los que se dirigen ataques, en los que España tiene una presencia variable (puesto 4 a 7). En Marzo de 2009, el número de ataques fraudulentos en España era el 25% del total. Y es que la banca electrónica, por ejemplo, continúa siendo uno de los usos on-line más generalizados entre los españoles. El número de usuarios de banca on-line en España ha experimentado en los últimos años una tendencia creciente, situándose a niveles parecidos a los del resto de países europeos. También encontramos a España en segunda posición en el mes de Marzo como país alojador de elementos o actividades fraudulentas.

Para INTECO, las actuaciones se centran en la atención, por un lado, a ataques a entidades españolas, y por el otro, a ataques que utilizan recursos ubicados en España. Entre las fuentes de información o detección de nuevos casos se utiliza de manera importante las propias denuncias de los usuarios. Cada vez se reciben más denuncias sobre otros tipos de fraude que hasta ahora eran menos conocidos que, por ejemplo, el phishing.

Incidentes y fraude en la red

Los defraudadores suelen utilizar variantes de ataques que afectan a la seguridad lógica del ordenador o el sitio web, como virus, ataques de denegación de servicio, sustracción de datos o cuentas de correo electrónico y suplantación de personalidad a través de medios telemáticos.

Además, intentan aprovechar todas las debilidades encontradas utilizando la ingeniería social basada en temáticas actuales y de gran impacto. La denominada "ingeniería social" es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían. Un ejemplo en la vida diaria es aplicado por un vendedor que investiga las costumbres y aficiones de un cliente para establecer una relación de confianza o empatía, poder vender con una mayor facilidad sus productos o servicios. La actual coyuntura económica provoca, pues, una explotación mayor de los recursos fraudulentos, pero no necesariamente provoca la aparición de nuevos recursos o nuevas técnicas: las viejas se adaptan a la realidad económica, política y social. Con la crisis y el creciente paro, por ejemplo, se ofrecen falsas y fraudulentas ofertas de trabajo, abriendo así un nuevo concepto en esta misma técnica aprovechando la incertidumbre económica.

Al parecer, a pesar de las recomendaciones que se realizan, el phishing a entidades financieras sigue siendo la mayor fuente de fraudes on-line (4 ataques distintos al mes). Recordemos que el phishing es la forma de ataque mediante la cual el ciber-delincuente trata de obtener información bancaria o financiera de la víctima, como claves personales, números de cuentas bancarias, etc. Existe diversas maneras de realizar un ataque: una puede ser enviándole al usuario un correo electrónico simulando ser un Banco en el que se le piden los datos personales utilizando alguna excusa del por qué se necesitan, para que lo responda o bien para que ingrese a algún link que simula ser la página del Banco pero que en realidad no lo es. Suelen ser ataques claramente planificados, dirigidos, sofisticados, dinámicos e inteligentes.

Pero no solamente las entidades financieras sufren este tipo de ataques. Para las empresas que necesitan transferir datos personales a través de la Web es vital ganarse la confianza de los clientes en línea. A los consumidores que compran en línea les preocupa el robo de identidad y, por tanto, se toman con mucha cautela el hecho de ofrecer sus datos personales (en especial los referidos a la tarjeta de crédito) a sitios que no sean de confianza. En otros tipos de negocios los datos que se transfieren, aunque no sean de carácter personal, también son importantes. Así las cosas, también cada vez más comercios, negocios, empresas o multinacionales son víctimas del fraude electrónico, o utilizadas para cometer, en su nombre y mediante correos o páginas web falsas con una alta ingeniería social y un diseño técnico convencional, actividades fraudulentas desde servidores situados fuera del país en el que se comete el fraude. La deslocalización para evitar la detección es habitual, cosa que dificulta el proceso de seguimiento a las autoridades competentes.

■ **D. Julio Cortés**
Centro Europeo del Consumidor (Instituto Nacional de Consumo)

Protección del consumidor en Europa: la red CEC

El Centro Europeo del Consumidor es una oficina pública de atención al consumidor de cualquier Estado Miembro de la Unión Europea que precise información o asistencia en relación con la adquisición de un bien o la utilización de un servicio en un país diferente al propio. Cualquier transacción transfronteriza es observada y analizada, y se facilita mediación en cualquier queja o reclamación transfronteriza. El objetivo es tratar de conseguir, mediante una labor preventiva e informativa, que en cualquier país europeo se tenga la certeza que los derechos de los consumidores serán reconocidos y garantizados.

El Centro Europeo del Consumidor en España puede ayudarle si:

• Es usted ciudadano de un estado comunitario que adquiere un bien o contrata un servicio en cualquier parte del territorio español

• Es usted un ciudadano español que adquiere un bien o contrata un servicio en un estado comunitario que no sea España

Parte del trabajo del Centro Europeo del Consumidor consiste en la difusión de información acerca de los derechos de los consumidores en la Unión Europea, así como de los retos a los que se enfrentan debido al avance, entre otras cosas, de las nuevas tecnologías. El aumento del número de transacciones por Internet provoca, de manera inevitable, que crezca también el número de quejas por fraude. En el 2007, el 56% de las reclamaciones europeas estaban relacionadas con el comercio electrónico, y la mayoría estaban basadas en términos de contratación confusos o deficientes, retrasos o extravíos en las compras realizadas a través de Internet, etc. Eso ha generado un alto grado de desconfianza en el usuario: el 27% realizan compras por Internet de manera habitual, pero el 70% de ellos no tiene la confianza necesaria cuando lo hace. Se debe dotar a los consumidores de confianza, ya que no obtienen suficiente información sobre las posibilidades que tienen de recuperar su dinero a través de los medios de pago. Un medio de pago seguro asegura también los derechos del consumidor.

Medios de Pago Seguros en Internet

La Comisión Europea tiene como objetivo la eliminación de cualquier barrera a los pagos transfronterizos y crear un espacio único de pago. Pero se ha podido constatar que en la actualidad estas transferencias continúan siendo más caras y lentas que las transferencias de dinero que se realizan dentro de un mismo Estado, ya que, a menudo, los sistemas de pago y las normas de seguridad de cada Estado no son compatibles. El poder, por ejemplo, retroceder los cargos realizados depende de la legislación de cada país y se exige demostrar claramente el fraude.

Los problemas detectados a lo largo del tiempo desde 2004 siguen persistiendo hoy en día. Una de ellas es la falta de claridad en páginas Web donde no se especifican bien las formas de pago, las medidas de contrato o el precio final del producto. Otra, probablemente una de las más importantes, es la poca educación de los consumidores contra el fraude y la falta del fomento del uso responsable de los medios de pago y los derechos del consumidor. Los consumidores por Internet no gozan de menos derechos que los consumidores tradicionales. Finalmente, destacar la necesidad de mecanismos eficaces de solución alternativa de conflictos en Internet.

Proyectos de cooperación europeos

El CEC pretende utilizar su conocimiento directo de los casos de fraude para llevar la problemática del consumidor más allá de la asistencia a los casos particulares. Para ello ha establecido reuniones periódicas con el sector empresarial dirigidas a observar la conformidad con la actual legislación en materia de protección a los consumidores. Asimismo, trabajará en estrecha colaboración con la Policía y otras instituciones nacionales e internacionales para mejorar esta protección mediante el intercambio fluido de información sobre malas prácticas comerciales.

El CEC organiza el Día del Barrido en Internet, basado en la revisión de páginas web de toda Europa de los temas que

generan actualmente más problemas, como el fraude en las ofertas de venta de billetes de avión. El barrido ha encontrado casos de publicidad engañosa y de incumplimiento de los requisitos legales establecidos para la venta de billetes de avión por internet. La búsqueda se ha realizado conjuntamente con otros países miembros de la Unión Europea en respuesta a iniciativas de organismos europeos de protección de los consumidores, comprobando siempre que en todos los países se cumple la normativa europea en materia de consumo y no se utilizan conceptos abusivos o se imponen condiciones abusivas.

Sistema de arbitraje electrónico en España: marco legal

En España, el BOE de 25/2/2008 publicó el Real Decreto 231/2008, de 15 de febrero, por el que se regula el Sistema Arbitral de Consumo. Y en los artículos 51 a 55 de dicho Real Decreto, se regula expresamente el Arbitraje de consumo electrónico.

El origen de esta regulación hemos de encontrarlo en el artículo 51 de la Constitución Española donde se insta a los poderes públicos a garantizar la defensa de los consumidores y usuarios, protegiendo mediante procedimientos eficaces, su seguridad, salud y sus legítimos intereses económicos. Igualmente, la Ley de 19 de Julio de 1984, General para la Defensa de los Consumidores y Usuarios, así como la recientemente publicada en Noviembre de 2005, preveían que el Gobierno debía establecer un sistema arbitral que, sin formalidades especiales, atendiera y resolviera con carácter vinculante y ejecutivo para ambas partes, las quejas y reclamaciones de los consumidores y usuarios. Por último, el Real Decreto 636/1993 de 3 de Mayo reguló el Sistema Arbitral de Consumo, y la Ley 44/2006 de 29 de Diciembre de mejora de la protección de los consumidores y usuarios, dejó previsto en su disposición final sexta que en plazo de un año desde su entrada en vigor, el Gobierno, contando con el parecer de las comunidades autónomas, dictará una nueva regulación del Sistema Arbitral de Consumo y regulará el arbitraje virtual.

En cumplimiento de estos mandatos, se promulga este decreto que en la parte que interesa, literalmente nos dice en su artículo 51: “El arbitraje de consumo electrónico es aquel que se sustancia íntegramente, desde la solicitud del arbitraje hasta la terminación del procedimiento, incluidas las notificaciones, por medios electrónicos, sin perjuicio que alguna actuación arbitral deba practicarse por medios tradicionales”.

En su artículo 53: “Firma electrónica. Sin perjuicio de la utilización de otras técnicas que aseguren la autenticidad de la comunicación y la identidad del remitente, el uso de la firma electrónica garantiza la autenticidad de las comunicaciones y la identidad de las partes y del órgano arbitral”.

Y en su artículo 54: “Las notificaciones se realizarán en la sede electrónica designada por las partes a tales efectos, entendiéndose realizadas a todos los efectos legales el día siguiente a aquél en que conste el acceso al contenido de la actuación arbitral objeto de notificación. No obstante, si el notificado no hubiera accedido al contenido de la actuación arbitral transcurridos diez días desde la fecha y hora en que se produjo su puesta a disposición, la notificación se considerará que se ha intentado sin efecto, procediéndose a la publicación edictal en las sedes electrónicas de las Juntas Arbitrales de Consumo adscritas al arbitraje de consumo electrónico”.

El futuro: Sistemas de resolución de conflictos on-line

Los sistemas on-line de resolución de conflictos son un producto de la popularización de los medios de comunicación en internet, que trajo el uso de correos electrónicos, entre otros, como un medio fácil, rápido y poco costoso. Otras herramientas, como el chat y el mensajero instantáneo han permitido la comunicación fácil y poco costosa a través del globo. Por otro lado, el mismo desarrollo del comercio on-line ha aportado un enorme número de transacciones entre comerciantes on-line y compradores on-line, de poco o mucho valor monetario, que han generado un alto número de disputas por resolver. Hay temas importantes y nuevos que se están generando ahora, a estudiar entre ellos como es posible crear confianza en la interacción inicial entre las partes, entre compradores y vendedores en el mundo electrónico, cuando estan a mucha distancia y sólo conectados por la pantalla del ordenador. La construcción de la confianza en el comerciante o proveedor de servicios on-line esta muy relacionada con que se ofrezca o no un procedimiento para que el cliente pueda hablar con la entidad y manifestar sus reclamaciones o quejas si algo falla en la transacción. Es vital para cualquier entidad el tener el feedback de sus clientes, y sin embargo esta posibilidad de ofrecer un canal para reclamaciones o quejas es todavía difícil de encontrar en el mundo del comercio electrónico, pese a que los sistemas de resolución de conflictos on-line son la actual tendencia en Europa. El futuro debe ser el sistema de arbitraje electrónico, que ya se aplica en algunos países como Italia, y que entre sus ventajas está el hecho de no tener que desplazarse geográficamente. La defensa de los consumidores se moderniza y se integra de pleno derecho en la sociedad de la información.

PARTE 4

Conclusiones y propuestas de ADICAE

CONCLUSIONES

■ Si algo se ha puesto de manifiesto a lo largo de todo el Simposium es el preocupante aumento de ataques, tanto en número como en diversidad, que los usuarios de medios de pago europeos sufren año a año. El principal objetivo de estos ataques es hacerse con datos personales, sobre todo los bancarios. El phishing e internet siguen siendo una de las principales armas de los delincuentes, aunque no hay que olvidar los cajeros automáticos y los comercios, donde también los delincuentes fijan sus objetivos, debido a la proliferación del uso de las tarjetas para cualquier tipo de pago.

■ También son preocupantes las técnicas cada vez más complejas y rápidas que utilizan los delincuentes, lo que indica los medios de los que disponen y su capacidad para evolucionar, dominar y evitar los medios tecnológicos y de seguridad que las empresas del sector les ponen como barrera.

■ La característica fundamental del fraude es su carácter transnacional, ya que éste fundamentalmente se produce a través de internet.

■ Se ha constatado la necesidad de comunicación entre los cuerpos policiales de diferentes países, que además necesitan de la colaboración de todo aquel que sufra o sepa de un fraude, puesto que sin denuncia no pueden perseguir al delincuente.

■ Es indispensable poner orden y coherencia entre la legislación en todos los países de la UE, tanto para la prevención como para el castigo de conductas delictivas referentes al fraude, en la actualidad no están armonizadas.

■ Es evidente cómo las entidades finacieras no son transparentes a la hora de hablar de fraude en medios de pago y no reconocen la gravedad de este problema. Según éstas no sufren a penas los efectos de estos, aunque las estadísiticas y datos de terceros no dicen lo mismo.

■ Ha quedado evidenciado quién sufre el impacto directo del fraude: el usuario. Éste sufre todos sus efectos, viéndose desprotegido por la propia entidad financiera, que no reconoce su responsabilidad y la deriva en su totalidad hacia el usuario amparándose en las cláusulas del contrato firmado.

PROPUESTAS

Por todo ello se constata que las medidas e iniciativas emprendidas hasta la fecha para prevenir y luchar contra el fraude y la falsificación de medios de pago distintos del efectivo no han resultado suficientes para atajar la difusión de este fenómeno. Son muchos los agentes que tienen relevancia en el sector de los medios de pago, y cada uno de ellos tiene su parte de implicación en el problema del fraude. Desde éstos se podrían lanzar diferentes medidas que atajarían el problema del fraude:

Entidades financieras

■ Aumentar los recursos destinados a la prevención del fraude en varios sentidos:

- Dotar de mejores medidas de seguridad sus medios de pago utilizados por sus clientes. Utilizando medios existentes que no se han generalizado: token usb para banca electrónica, utilización de tarjetas de coordenadas para sus clientes de banca electrónica, doble vía de validación de operaciones (por medio de teléfono móvil), etc.
- Fomentar la cultura de la seguridad: Entre sus empleados, mediante cursos de formación, y entre sus clientes con campañas formativas, publicaciones, etc.

■ Compromiso de revisión por parte de organismos de control financieros (Bancos Nacionales) de sus contratos de medios de pago para la eliminación de cláusulas abusivas que en la actualidad dejan en indefensión al consumidor en situaciones de fraude.

Poder Judicial

■ Formación contínua sobre este tema a través de Escuelas Judiciales y Centros de Estudios Jurídicos

■ Cooperación y colaboración con Cuerpos Policiales y Administración competentes en la materia.

Emisores y empresas de seguridad especializadas. Deben trabajar principalmente en dos frentes

■ La prevención del fraude (desarrollando parches de seguridad que minimicen las posibles vulnerabilidades de los sistemas operativos y programas informáticos y prestando servicios a las propias entidades financieras con sistemas de filtrado del tráfico, de protección ante intrusiones, detección de webs fraudulentas, etc.);

■ La investigación e innovación tecnológica colaborando con otros agentes implicados como son los Cuerpos y Fuerzas de Seguridad del Estado.

Comercios y empresas que operan a traves de internet

■ Incidir en la seguridad como un aspecto fundamental del negocio por internet

■ Considerar los recursos destinados a proteger la seguridad de las comunicaciones como una inversión

■ Considerar la seguridad como un aspecto de la calidad del servicio

■Plan de formación de sus empleados en materia de seguridad y protección de datos personales, llegando a implantar una "cultura de la seguridad"cos (revisión del cajero y en caso de sospechar no utilizarlo y comunicarlo a la entidad);

Consumidores

■ Mayor exigencia propia a la hora de utilizar los medios de pago: actualización periódica de medidas y herramientas de seguridad informática (antivirus, cortafuegos, etc), precaución a la hora de utilizar cajeros automáticos (revisión del cajero y en caso de sospechar no utilizarlo y comunicarlo a la entidad);

■ Utilización del DNI electrónico para la validación y confirmación de sus operaciones a través de internet.

■ Precaución. En el caso de realizar una operación y tener sospechas desistir de hacerla, en caso de haberla realizado denunciar el hecho lo más pronto posible en la comisaría más cercana.

■ Exigir seguridad al suministrador del servicio. Demandar medidas de seguridad que le hagan a él confiar en el servicio.

Asociaciones de consumidores

■ Emprender campañas informativas precisas de gran difusión 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.

■ Colaboración con Administración y Cuerpos Policiales, tanto para la transmisión de conocimientos y experiencias a sus asociados como para la denuncia de casos recibidos por éstas.

ADICAE

al servicio de los usuarios en toda España y en Europa

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 - 2ºC - 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

ANEXO

Transposición de la Directiva de servicios de medios de pago en la U.E.

TRANSPOSICIÓN DE LA DIRECTIVA DE SERVICIOS DE MEDIOS DE PAGO EN LA U.E.

Estado Miembro	Situación	Fecha esperada de adopción	Fecha esperada de entrada en vigor
Bélgica	Un grupo de trabajo creado especialmente a tal efecto que engloba a todas las autoridades competentes involucradas (Ministerios afectados, NBB, Comisión Bancaria, financiera y de Seguros) se ha puesto en marcha. La autoridad supervisora (CBFA) será, siguiendo la supervisión del Ministerio de Economía, responsable de la implementación del Título II; mientras que los Títulos III y IV recaerán dentro de la responsabilidad de los Ministerios de Economía, además del Ministerio de Finanzas y de Protección del Consumidor. Se publicó el borrador de la Ley a finales del 2008, y se recibieron las alegaciones de los distintos agentes. Se enviará el borrados en la segunda mitad del 2009. No se ha previsto ninguna consulta pública.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Bulgaria	La Ley sobre Servicios y Medios de Pago, que transpone la Directiva sobre Medios de Pago, se publicó en el Boletín Oficial nº 23 el 27.3.2009, y puede consultarse en http://dv.parliament.bg/.	27.3.2009	1 de Noviembre de 2009
República Checa	El trabajo en cuanto a la transposición ha avanzado. El Ministerio de Finanzas ha dirigido el proceso, en cooperación con el Banco Nacional de la República Checa. El Borrador elaborado per el Ministerio está siendo actualmente consultado por comités legislativos del Gobierno; el borrador de la Ley no será enviado al Parlamento hasta finales de Abril de 2009, y no se podría ser aprobado por el Parlamento en Agosto de 2009.	4º Cuatrimestre 2009 (Octubre)	1 de Noviembre de 2009
Alemania	La Ley que implementa la parte supervisoria de la Directiva sobre Medios de Pago ha sido adoptada por el Gobierno Federal el 26 de Marzode 2009. Será llevado al Parlamento Federal para que se apruebe. Respecto a la Ley que implementará la parte civil de la Directiva, se llevó a cabo una audiencia pública en el Parlamento Federal el 23 de Marzo de 2009. Esta Ley se espera que sea adoptada en Mayo o Junio antes de ser enviada al Consejo Federal. Ambos procesos de tranposición se espera que se terminen antes de las vacaciones de verano.	2º Cuatrimestre 2009	31 Octubre 2009
Estonia	Los trabajos en cuanto al borrador para la Ley que transpone la Directiva están siendo dirigidos por el Ministerio de Finanzas. Los títulos III y IV están siendo tratados conjuntamente con el Ministerio de Justicia. La preparación de el borrador se consulta en cooperación con el Banco de Estonia y autoridad de servicios financieros. El objetivo es tener listo el Proyecto de Ley para consulta pública en Abril de 2009 y enviarla para su aprobación al Gobierno en Mayo de 2009 como muy tarde, tras lo que se enciará al Parlamento.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Irlanda	Los trabajos para la transposición ya han comenzado. El Departamento de Finanzas y el Banco Central, además de la Autoridades de Servicios Financieros en Irlanda están trabajando en cooperacion con los legisladores del estado para finalizar el proceso de transposición. Se planea llevar a cabo una consulta concurrente del Borrador de la legislación con los principales atgentes interesados, incluyendo la cuestión de la migración a Débito Directo. La consulta se llevará a cabo dirante el Verano (Julio, Agosto)	Tercer Cuatrimestre de 2009 (Septiembre)	1 de Noviembre de 2009
Grecia	La Decisión del Ministerio de Finanzas nº 9989/B504/29.2.2008 estableció un Comité para la redacción del Proyecto de Ley. Los miembros de este Comité para la Transposicion representan a autoridades públicas, reguladores y sector privado. Hasta la fecha, este Comité se ha reunido nueve veces y ha acabado la prmera lectura del Proyecto de Ley. El Proyecto se terminó a mediados de Febrero de 2009, y fue consecuentemente enviado para consulta pública de todos los interesados en este tema (instituciones financieras, asociaciones de consumidores, cámaras de comercio, etc.) Hay dos cuestiones claves todavía en discusión: – La aplicación del Título IV de la Directiva a pequeñas empresas y a consumidores (Artículo 30, párr. 2 y Art 51, párr. 3) – la obligación de migrar los pagos realizados mediante las transacciones de débito directo	2º Cuatrimestre 2009	1 de Noviembre de 2009

España	El Consejo de Estado acaba de publicar el informe sobre el Borrador de Ley. El Consejo de Ministros enviará el texto al Parlamento en Abril	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Francia	Los grupos de trabajo formados a tal efecto con representantes del Banco Nacional de Francia, los ministerios relevantes, federaciones bancarias proveedores de servicios de telecomunicación, etc. ya se han reunido varias veces. Un Decreto para autorizar al Gobierno para transponer la Directiva a través de una Ordenanza se aprobó el 5 de Agosto. Se inició una Consulta Pública el 3 de Septiembre de 2008 y se acabóo el 21 ede Octubre de 2008. El Proyecto de Ley se enviará al Consejo de Estado en Abril y la Ordenanza se espera que sea adoptada por el Gobierno antes de Verano.	Segundo Cuatrimestre 2009	1 de Noviembre de 2009
talia	El trabajo para la Transposición ya ha comenzado. Un Grupo de Trabajo formado por el Ministerio de Economía, supervisores, Banco Central y representantes de la Banca se ha formado, y se añadirán representantes si es necesario.Se espera que el Parlamento apruebe la Ley para el final de Abril. El Decreto Legislativo (ley primaria) de la transposición será aprobado por el Gobierno durante el verano, y en cualquier caso, como muy tarde Noviembre de 2009.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Chipre	El banco Central Nacional era el responsable de la preparación del Proyecto de Ley. Este trabajo se ha llevado a cabo con la cooperación del Ministerio de Finanzas. Otras partes interesados en este tema involucrados en el Grupo de Trabajo eran las cooperativas sociales, la autoridad de supervisión y desarrollo ademas del Ministerio de Comercio, Industria y Turismo. Todos los demás interesados están representados en un comité para la adaptación a la SEPA. Se inició una consulta pública el 17 de diciembre de 2008 sobre el borrador de Ley para la SEPA. were the Co-operative Societies Se inició una consulta pública el 17 de Diciembre de 2008 sobre el borrador de Ley y el segundo borrador legislativo (las provisiones de la transposición del Banco Central de Chipre contenidas en el Título II y el art.88) transpondrá la Directiva a la normativa chipriota. Ambos borradores están disponible en la página web del Ministerio de Finanzas (www.mof.gov.cy) de manera conjunta con comentarios.Se recibieron los comentarios de seis interesados en la materia dentro del plazo (30 Enero 2009). Además, una petición del Ministerio de Finanzas para una opinión del BCE sobre el Borrador de Ley se remitión el 5 de Mayo de 2009. El objetivo es que se pueda enviar el Borrador de Ley al Parlamento de Chipre en Primavera de 2009, de tal forma que se permita ek procedimiento habitual en el Parlamento.	Cuarto Cuatrimestre 2009 (Octubre)	1 de Noviembre de 2009
Letonia	El Ministerio de Finanzas ha empezado la implementación. No se ha establecido formalmente ningún grupo de trabajo, pero ha habido cooperación entre el Ministerio, Banco Central y autoridad en servicios financieros	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Lituania	Están actualmente disponibles para consulta pública los borradores de Ley que transponen la Directiva; están disponibles en http://www.finmin.lt/web/finmin/teises_aktai/rengiami?erp_item=rengiami_teises_aktai_000154. La consulta pública durará al menos hasta finales de Abril. Está previsto que los Borradors se lleven al Parlamento en Junio. La adopción tal vez se produzca en Julio.	Tercer Cuatrimestre de 2009 (Julio)	1 de Noviembre de 2009
Luxemburgo	El borrador de Ley ha sido aprobado por el consejo de gobierno el 6 de Marzo y se ha enviado al Parlamento y al Consejo de Estado. El objetivo sigue siendo que la Ley se adpote antes del 1 de Noviembre de 2009.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Hungary	Un Comité especial sobre asuntos políticos adoptó el primer borrador sobre la Ley de Servicios de Pago, la cual será el principal instrumento para la transposición de la Directiva (además de legislación complementaria: un Decreto del Gobierno y otro del Banco Central) el 12 de Diciembre. Este borrador está disponible para ser descargado en la web del Ministerio (http://www1.pm.gov.hu/) desde el 19 de Diciembre hasta el 9 de Enero. Se espera que se envíe el borrador al Parlamento a principios de Abril.	Segundo Cuatrimestre 2009	1 de Noviembre de 2009

Malta	El Banco Central ha supervisado la transposición y coopera con las autoridades de servicios financieros de Malta (responsables del Título II) y con la Oficina para la Supervisión de la Libre Competencia. Después de publicar un documento consultivo extraido de un extenso proceso de consulta pública, el Banco Central de Malta ha publicado un resumen de las respuestas recibidas (disonible en www.centralbankmalta.org), y un comité conjunto formado por las autoridades de servicios financieros y el Banco Central de Malta están teniendo en cuenta los resultados de ese proceso y las conclusiones del Grupo para la transposición de la Directiva. A pesar de que se espera que gran parte de la Directiva tomará efecto a causa de la aprobación de leyes complementarias propuestas por las autoridades de servicios financieros y Banco Central a través de la Resolución de Instituciones Financieras y la Resolución del Banco Central de Malta respectivamente, otra Ley para que entren en vigor ciertas enmiendas de estas ordenanzas se envíen ante el Parlamento hacia finales de Abril.	Segundo Cuatrimestre 2009	1 de Noviembre de 2009
Holanda	El Ministerio de Finanzas holandés ha escrito un borrador de enmienda de la Ley de Supervisión Financiera y Código Civil. El pasado verano, las partes interesadas fueron consultadas sobre el borrador. La Ley fue enviada al Parlamento. La Cámara Baja probablemente trate sobre esta cuestión antes de verano; y la Cámara Alta se ocupará de ello en el tercer cuatrimestre del año. Tendrá lugar una consulta sobre legislación complementaria durante el segundo cuatrimestre de 2009.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Austria	El borrador de Ley ha sido enviado para consulta formal en Enero de 2009 (https://www.bmf.gv.at/Finanzmarkt/RechtlicheGrundlage_753/Zahlungsdienstegesetz/_start.htm); la consulta estuvo abierta hasta finales de Febrero. Se enviará el borrador final al Parlamento después de Semana Santa.	Segundo Cuatrimestre 2009	1 de Noviembre de 2009
Polonia	La consulta pública de la implementación de la Directiva se iniciará en Abril	Segundo Cuatrimestre 2009	1 de Noviembre de 2009
Portugal	Un primer borrador se ha enviado ya al Ministerio de Finanzas y se ha enviado también para la consulta. La consulta pública se ha finalizado y el Ministerio de Finanzas pronto recibirá una propuesta dinal que será decidida y para el final de ese proceso se enviará para su aprobación al Gobierno.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Romania		Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Eslovenia	El borrador de Ley ha sido aprobado por el consejo de gobierno el 6 de Marzo y se ha enviado al Parlamento y al Consejo de Estado. El objetivo sigue siendo que la Ley se adpote antes del 1 de Noviembre de 2009.	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Eslovaquia	El borrador legislativo que propone la Directiva está disponible a través de los comentarios sobre el procedimiento en la web del Ministerio de Finanzas de la República Eslovaca en http://www.finance.gov.sk/Default.aspx?CatID=7209 y además en el Portal de Legislación del Ministerio de Justicia de la República Eslovaca en https://lt.justice.gov.sk/(X(1)S(2twtim45suofcnf02gawma2m))/Material/MaterialHome.aspx?instEID=-1&matEID=1267&langEID=1.	Segundo Cuatrimestre de 2009	1 de Noviembre de 2009
Findlandia	Dos grupos de trabajo fueron establecidos: uno con el Ministerio de Justicia (trabaja en los Títulos III y IV), uno con el Ministerio de Finanzas (resto de la Directiva). Todos los agentes interesados relevantes están representados (incluyendo sector de telecomunicaciones y consumidores). El borrador de Ley preparado por el Ministerio de Justicia está disponible en la web del Ministerio. La Propuesta de Ley, que será preparada por el Ministerio de Finanzas, debería estar preparada para mediados de Mayo. La consulta oficial de ambos borradores debería tener lugar a principios de Verano. Los borradores de Ley deberían de ser enviados al Parlamento en Octubre de 2009.	Cuarto Cuatrimestre de 2009	1 de Noviembre de 2009
Suecia	Existe el riesgo de que Suecia no pueda implementar la Directiva antes del 1 de Noviembre. De acuerdo con el calendario revisado, se espero enviar una propuesta al Parlamento en Diciembre.		1 de Noviembre de 2009

Suecia	Existe el riesgo de que Suecia no pueda implementar la Directiva antes del 1 de Noviembre. De acuerdo con el calendario revisado, se espero enviar una propuesta al Parlamento en Diciembre.	?	?
Reino Unido	La normativa que implementala Directiva entró en vigor el 2 de Marzo de 2008. Se publicó el 12 de Febrero de 2009 un resumen de respuestas a la consulta pública sobre el borrador legislativo, además de un memorándum explicativo a las regulaciones. Estos documentos se pueden encontrar en http://www.hm-treasury.gov.uk/fin_payment_index.htm. Las autoridades de servicios financieros publicaron una consulta sobre sus reglas para establecer un sistema de reclamación extrajudicial y de reclamación en Agosto de 2008, y se espera que publique las reglas finales en Marzo de 2009- Además de la dimensión territorial de las medidas adoptadas, está todavía considerándose si se necesitaría legislación adicional para Gibraltar y las islas del Canal de La Mancha. La Autoridad en Servicios Financieros ha publicado un documento de acercamiento, guía y sus políticas para ayudar a las empresas a entender los requerimientos de la Directiva, y qué necesitan preparar para Noviembre. Los documentos se pueden consultar en http://www.fsa.gov.uk/Pages/About/What/International/psd/.	2 Marzo 2009	Implementación final:1 Noviembre 2009

PAÍSES DEL ÁREA ECONÓMICA EUROPEA

Islandia	Aún no se dispone del borrador de la Directiva 2007/64/EC	Tercer /Cuarto Cuatrimestre de 2009	1 de Noviembre de 2009
Liechtenstein	El Borrados se formalizó durante el tercer cuatrimestre de 2008; el borrador final listo en el segundo cuatrimestre de 2009	Tercer Cuatrimestre de 2009	1 de Noviembre de 2009
Noruega	El grupo de trabajo dedicado a la transposición con representantes de los Ministerios implicados, el banco Central, Autoridad de Servicios Financieros, consumidores e industria entregó su primer informe sobre los Títulos III y IV en Febrero de 2009, y se ha llevado a cabo una audiencia pública. El informe y la respuesta pueden encontrarse en http://www.regjeringen.no/nb/dep/jd/dok/hoeringer/hoeringsdok/2009/horing---forslag-til-gjennomforing-avbe.html?id=546595. El Ministerio de Justicia propondrá enmiendas para la Ley de contratos Financieros para transponer los títulos III y IV en breve- El Parlamento Noruego probablemente revisará la Ley antes de su descanso estival. El grupode trabajo espera entregar un informe sobre el Título II al Ministerio de Finanzas en primavera de 2009.	Segundo Cuatrimestre de 2009	1 de Noviembre de 2009

Fuente: Comisión Europea, DG Internal Market, http://ec.europa.eu/internal_market/payments/framework/transposition_en.htm