

Iniciativas para fomentar el uso de los servicios bancarios a distancia

La banca a distancia, y especialmente la banca online, se ha desarrollado al ritmo de la profundización en la Sociedad de la Información en España, hasta consolidarse como un canal esencial para la distribución de servicios financieros. Cuatro factores han facilitado esta situación: los cambios normativos y regulatorios, los desarrollos tecnológicos del mercado, las mejoras en el acceso y uso y en la funcionalidad ofrecida y, por último, las mejoras en la seguridad de los canales electrónicos. Este artículo hace un repaso de los cuatro pilares que configuran el entorno propicio y señala algunas de las tendencias para los próximos años.

Urrutiko bankua, eta batez ere online bankua, Espainian Informazio Gizartean sakondu den erritmo berean garatu da, finantza-zerbitzuak banatzeko ezinbesteko bide gisa finkatu arte. Lau izan dira egoera hau erraztu dutenak: arauetan eta erregulazioan eman diren aldaketak, merkatuaren garapen teknologikoak, eskuraketan eta erabileran baita eskainitako funtzionalitatean ere izandako hobekuntzak eta, azkenik, bide elektronikoen segurtasunean gertatuako hobekuntzak. Artikulu honek inguru egokia prestatzen duten lau euskarrien berrikusketa bat egiten du eta datorren urtetarako joera batzuk aipatzen ditu.

Online banking has developed at the same pace as the Information Society in Spain, it is fast becoming an essential channel for the distribution of financial services. Up to four different factors have eased this situation: legal and regulatory changes, recent technological developments, improvements in usability and functionality and, finally, improvements in security measures for electronic channels. This article reviews the four pillars that configure this favourable environment and points out some future trends.

ÍNDICE

1. Introducción
 2. Las novedades que provienen de la regulación: nueva normativa para el impulso de la sociedad de la información
 3. Las novedades que proceden del mercado: movilidad y Web 2.0
 4. Las novedades fruto de la evolución de las funcionalidades de la banca online: ¿cómo mejorar la experiencia de usuario?
 5. Las novedades que surgen del ámbito de la seguridad: iniciativas para identificar a los usuarios e iniciativas para defenderse de los ataques
 6. Conclusiones
- Referencias bibliográficas

Palabras clave: Sociedad de la Información, banca a distancia, banca online, banca móvil, innovación

Keywords: online bank, phishing, mobile bank, digital signature

N.º de clasificación JEL: L86, G21 y O33

1. INTRODUCCIÓN

España se encuentra inmersa en un proceso de profundización en la Sociedad de la Información (SI) que no tiene precedentes. Uno de los sectores económicos que lidera este proceso, y en el que los esfuerzos se ponen de manifiesto de una forma más patente, es el de los servicios bancarios. No obstante, lejos de poder explicar este fenómeno observando exclusivamente los desarrollos tecnológicos del propio sector financiero, es necesario tener en consideración diversos factores que lo han hecho posible. Así, el análisis sistemático de la explosión de la banca a distancia debe con-

templar al menos cuatro pilares: las modificaciones en la regulación, los desarrollos del mercado, los avances en la usabilidad y en la funcionalidad ofrecida por las entidades de crédito y las mejoras en la seguridad del uso de Internet.

Este artículo hace un repaso de los cuatro pilares mencionados, comenzando por el más amplio de la regulación, que no se circunscribe exclusivamente al sector financiero, para finalizar con el de la seguridad. Si bien se ha tratado de describir este último de forma objetiva y técnica, no debemos olvidar que incorpora un componente de percepción y subjetividad por parte del

cliente de servicios bancarios a distancia sobre el que no nos consta que se hayan desarrollado iniciativas relevantes; sin embargo, es esencial para el impulso definitivo a la Sociedad de la Información.

2. LAS NOVEDADES QUE PROVIENEN DE LA REGULACIÓN: NUEVA NORMATIVA PARA EL IMPULSO DE LA SOCIEDAD DE LA INFORMACIÓN

2.1. Plan Avanza

España cuenta con un plan director para el desarrollo de la Sociedad de la Información y de convergencia con Europa denominado Plan Avanza, cuyo titular es la Secretaria de Estado de Telecomunicaciones y para la SI, integrado en el programa de reformas para cumplir con la renovada

Estrategia de Lisboa del año 2005, cuyos objetivos están orientados al crecimiento económico y a la creación de empleo. Desde un punto de vista global, el Plan Avanza se integra dentro del objetivo estratégico de impulso a la Investigación + Desarrollo + innovación (Programa Ingenio 2010). Ver gráfico n.º 1

No obstante, previo a la aprobación del español Plan Avanza se desarrolló una Ponencia dentro del Consejo Asesor de Telecomunicaciones y Sociedad de la Información (CATSI) cuyas recomendaciones (junio de 2005) ayudaron a elaborar sus premisas, elementos y objetivos:

- Las tecnologías de la información y las telecomunicaciones (TIC) constituyen la clave del crecimiento económico y de la mejora de la productividad y la competitividad.

Gráfico n.º 1

Plan Nacional de Reformas

1. Refuerzo de Estabilidad Macroeconómica presupuestaria
2. Plan Estratégico de infraestructuras y Transporte y Programa de Agua
3. Aumento y mejora del Capital Humano
4. Estrategia I+D+I (Ingenio 2010)
5. Más competencia, mejor regulación, eficiencia de las AAPP y Competitividad
6. Mercado de trabajo y diálogo social
7. Plan de fomento empresarial

Ingenio 2010

Fomento de la innovación tecnológica y Sociedad de la Información

- AVANZA@: Potenciar la Sociedad de la Información
- CENIT: aumentar la colaboración público-privada en I+D+I
- CONSOLIDER: conseguir la excelencia investigadora

**plan
avanza**

Fuente: Plan Avanza

- Se debe hacer una política inclusiva, para mejorar la calidad de vida y aumentar la cohesión social.
- La elaboración y el desarrollo de un plan con estas características es una tarea común que requiere de la participación y el esfuerzo de toda la sociedad española.
- El Plan se fundamenta en la iniciativa europea «2010: Una Sociedad de Información Europea para el crecimiento y el empleo», presentada por la Comisión Europea el 31 de mayo de 2005.

De acuerdo con su enunciación de objetivos, el Plan Avanza se orienta a conseguir la adecuada utilización de las TIC para contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional y la mejora del bienestar y la calidad de vida de los ciudadanos, estructurándose en torno a cinco grandes áreas de actuación:

1. *Ciudadanía Digital, (hogar e inclusión de ciudadanos)*, donde se desarrollan medidas para garantizar la extensión del uso de las TIC en los hogares y para aumentar y potenciar la inclusión; además, se amplían los ámbitos de participación de la ciudadanía en la vida pública, cuyos objetivos son:
 - Aumentar la proporción de hogares equipados y que usan las TIC de forma cotidiana.
 - Incrementar el conocimiento de los beneficios de la SI entre los ciudadanos, así como la proporción de personas que utilizan las TIC en su vida diaria.
2. *Competitividad e Innovación*, con medidas encaminadas a impulsar el desarrollo del sector TIC en España y la adopción de soluciones tecnológicamente

avanzadas por las pymes españolas. Esta área de actuación persigue incrementar el grado de adopción de las TIC por parte de las pymes en los procesos de negocio. Un ejemplo sería la conexión a la banda ancha o impulsar la implantación de la factura electrónica.

3. *Economía Digital (educación en la era digital)*, incorporando las TIC en el proceso educativo y formativo e integrando a todos los agentes que en él participan.
4. *Servicios Públicos Digitales*, con medidas que permitan mejorar los servicios prestados por las Administraciones Públicas, aumentando la calidad de vida de los ciudadanos y la eficiencia de las empresas, que tiene como metas:
 - Conseguir una Administración Electrónica completamente desarrollada.
 - Garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las Administraciones Públicas.
 - Transformar una educación basada en modelos tradicionales en una educación cimentada en la SI.
5. *Contexto Digital*, con el despliegue de infraestructuras de banda ancha que lleguen a todo el país, genere confianza en ciudadanos y empresas en el uso de las nuevas tecnologías, proporcione mecanismos de seguridad avanzados y promueva la creación de nuevos contenidos digitales. El objetivo de este Contexto Digital es:
 - Extender las infraestructuras de telecomunicaciones en áreas con demanda desatendida.
 - Extender la banda ancha y la movilidad.

- Aumentar el grado de concienciación, formación y sensibilización de los ciudadanos, empresas y Administraciones Públicas, en materia de seguridad de las TIC.
- Impulsar la identidad digital.

En línea con las áreas de actuación, este Plan se acompañará de reformas normativas para incrementar el desarrollo de la Sociedad de la Información, para eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva SI.

Actualmente las piezas angulares de nuestro marco jurídico en cuanto al desarrollo de la SI son:

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.

Que se complementan, aunque de forma indirecta, con:

- Ley 32/2003, de 3 de noviembre, y Ley 11/1998, de 24 de abril, General de Telecomunicaciones.
- Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista.

Si bien la mayoría de la normativa no se ha aprobado bajo el paraguas del Plan Avanza, ha sido actualizada y puesta al día por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LISI), lo que nos permite considerarla como el elemento central de toda nuestra normativa en materia de Sociedad de la Información.

2.2. **Ley de Medidas de Impulso de la Sociedad de la Información**

Principales novedades de la Ley

La Ley de Medidas de Impulso de la Sociedad de la Información se organiza en torno a 2 capítulos. El capítulo I de la Ley introduce los preceptos dirigidos a impulsar el empleo de la factura electrónica y el uso de medios electrónicos en todas las fases de los procesos de contratación, así como a garantizar una interlocución electrónica de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica. Las principales aportaciones se dan en las siguientes áreas:

—*Facturación electrónica.* La Ley establece la obligatoriedad del uso de la factura electrónica en la contratación con el sector público estatal y define el concepto legal de factura electrónica como «un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor». Así se establece que en un plazo máximo de 6 meses desde la publicación de la Ley, el Ministerio de Industria, Turismo y Comercio y el Ministerio de Economía y Hacienda aprobarán las normas sobre formatos estructurados estándar de facturas electrónicas, mientras que en 9 meses el Gobierno establecerá un plan para la generalización del uso de la factura electrónica en España.

—*Firma electrónica.* La LISI establece la obligación de las empresas de sectores con especial incidencia en la actividad económica de facilitar un medio de interlocución telemática a los usuarios que cuenten con certificados

reconocidos de firma electrónica. De esta manera, se trata de asegurar que los ciudadanos cuenten con un canal de comunicación electrónica con las empresas cuyos servicios tienen una mayor trascendencia cotidiana. A tales efectos, se especifica que dicha interlocución telemática debe facilitar al menos la realización de trámites tales como:

1. La contratación electrónica, modificación de condiciones contractuales, finalización o rescisión.
2. La consulta de datos de cliente incluyendo un histórico de facturación de los últimos 3 años.
3. La presentación de quejas, incidencias y reclamaciones, garantizando la constancia de su presentación.
4. El ejercicio de derechos de acceso, rectificación, oposición y cancelación en materia de protección de datos.

En este sentido, tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica las que agrupen a más de cien trabajadores o aquéllas cuyo volumen anual de operaciones exceda de 6 millones de euros. En particular, aquí se han de incluir aquellas empresas que ofrecen servicios financieros destinados a consumidores: servicios bancarios, de crédito o de pago, servicios de inversión, operaciones de seguros privados, planes de pensiones y la actividad de mediación de seguros. No obstante, el citado precepto no impide que, excepcionalmente, las empresas obligadas por dicho precepto no faciliten la contratación de productos o servicios que, por su naturaleza, no sean susceptibles de comercialización por vía electrónica.

En esta línea y aprovechando las ventajas del DNI electrónico (DNle), Caixa Galicia se ha convertido a principios de marzo de

2008 en la primera entidad de crédito española en permitir que parte de sus contratos se firmen mediante el uso de este documento de identificación, sin necesidad de desplazarse a la sucursal para rubricar dichos contratos. Para ello emplea tecnología de firma electrónica y archivo totalmente española y con plena validez jurídica.

—Ofertas públicas de contratación electrónica entre empresas. La Ley define oferta pública de contratación electrónica entre empresas (B2B) como el proceso electrónico total, abierto y limitado en el tiempo, por el que una empresa ofrece la posibilidad de comprar o vender un determinado tipo de productos a otras empresas de manera que la contratación final se adjudique a la propuesta mejor valorada. Igualmente, se definen los requisitos para que sea calificada «Oferta pública de contratación electrónica de transparencia garantizada». Por su idoneidad en los procesos de contratación pública, el Gobierno promoverá la contratación electrónica de transparencia garantizada en sus relaciones comerciales.

El capítulo II de la Ley engloba las modificaciones legislativas que se han estimado necesarias para promover el impulso de la SI y de las comunicaciones electrónicas.

Modificaciones a la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

Las modificaciones que afectan a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)-tienen como finalidad, entre otras:

—Introducir obligaciones en materia de transparencia de precios: cuando el servicio de la SI haga referencia a precios, se facilitará información clara y

- exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o sobre aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.
- Flexibilizar las obligaciones referidas a las comunicaciones comerciales y a la contratación electrónica a fin de, entre otras razones, adecuar su aplicación al uso de dispositivos móviles (teléfonos, agendas electrónicas...).
 - Suprimir la obligación acerca de la constancia registral de los nombres de dominio, dado que se ha revelado como poco operativa desde un punto de vista práctico.
 - Establecer obligaciones de información sobre seguridad: la obligación de los proveedores de acceso a Internet establecidos en España de informar a sus usuarios sobre los medios técnicos que permitan, entre otros, la protección frente a virus informáticos y programas espía, la restricción de los correos electrónicos no solicitados, y la restricción o selección del acceso a determinados contenidos y servicios no deseados o nocivos para la juventud y la infancia. Se obligará igualmente a dichos prestadores, así como a los prestadores de servicios de correo electrónico, a informar a sus clientes sobre las medidas de seguridad que aplican en la provisión de sus servicios. Se encomendará a los proveedores de servicios de acceso la función de informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos; en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.
 - Precisar la responsabilidad del proveedor del enlace (*link*) o del motor de búsqueda de los contenidos de los que tiene conocimiento cuando hayan sido elaborados bajo su «dirección, autoridad o control».
 - Facilitar el acceso a los códigos de conducta por vía electrónica, fomentándose su traducción a las distintas lenguas oficiales del Estado y de la Unión Europea con el fin de proporcionarles la mayor difusión posible.
 - Flexibilizar la exigencia de información sobre mensajes publicitarios a través de correo electrónico o medios de comunicación equivalentes de modo que, en lugar de la inserción del término «publicidad» al inicio del mensaje, pueda incluirse la abreviatura «publi». Se trata de una medida que ha sido solicitada en diversas ocasiones por agentes que desarrollan actividades relacionadas con la publicidad a través de telefonía móvil y, por otra parte, no supone menoscabo de la protección y de los derechos de información de los usuarios, ya que el término «publi» es fácilmente reconocible como indicativo de «publicidad».

Modificaciones a la Ley de Firma Electrónica

Las más destacadas modificaciones que afectan a la Ley 59/2003, de 19 de diciembre, de Firma Electrónica son:

- Establecer obligaciones de información previas a la contratación mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita. Dicha información debe ser clara, comprensible e inequívoca e incluir:
 1. Los distintos trámites que deben seguirse para celebrar el contrato.

2. Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.
 3. Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos.
 4. La lengua o lenguas en que podrá formalizarse el contrato.
- Flexibilizar las obligaciones de información previa en materia de contratación electrónica para ponerla a disposición de los usuarios «mediante técnicas adecuadas al medio de comunicación utilizado», con vistas a facilitar la realización de operaciones de contratación electrónica mediante dispositivos que cuenten con pantallas de visualización de formato reducido.
 - Entender cumplidas las obligaciones de información previa cuando el prestador facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario en los casos en los que el citado prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido.
 - Definir «documento electrónico» para alinearlos en mayor medida con los conceptos utilizados en otras normas españolas de carácter general y en los países de nuestro entorno como la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.
 - Aceptar el especial valor probatorio de los contratos electrónicos que se rea-

licen mediante el uso de instrumentos de firma electrónica.

Modificaciones a la Ley de Ordenación del Comercio Minorista

Debemos mencionar que, entre las modificaciones que afectan a la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, se introduce un nuevo tipo de infracción a fin de respaldar la nueva obligación de disponer de un medio de interlocución electrónica para la prestación de servicios al público de especial trascendencia económica.

Modificaciones a la Ley General de Telecomunicaciones

Las novedades más relevantes que afectan a la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones son las siguientes:

- Garantizar que todos los usuarios finales puedan obtener una conexión a la red pública desde una ubicación fija y acceder a la prestación del servicio telefónico. La conexión debe ofrecer al usuario la posibilidad de efectuar y recibir llamadas telefónicas y permitir comunicaciones de fax y datos de velocidad suficiente para acceder a Internet, debiendo permitir dicha conexión las comunicaciones en banda ancha en los términos definidos por la normativa.
- Instar a que la autoridad de asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España (».es») adopte las medidas que sean necesarias para asegurar que puedan asignarse nombres de dominio que contengan caracteres propios de las lenguas oficiales de España distintos de los incluidos en el alfabeto inglés, como es la letra «ñ» o la «ç».

- Impulsar la extensión de la banda ancha con el fin de conseguir antes del 31 de diciembre de 2008 una cobertura de servicio universal de banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada (en su caso) y de su ubicación geográfica.
- Analizar de forma continua las diferentes opciones tecnológicas y las condiciones de provisión de servicios de acceso a Internet de banda ancha. Para ello, se colaborará con los diferentes sectores interesados a fin de que asesoren al Gobierno en la elaboración de un informe anual sobre la situación del uso de los servicios de acceso a Internet de banda ancha en España, que tendrá carácter público.
- Elaborar un Plan para la mejora de los niveles de seguridad y confianza en Internet, que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad *online*.
- Asignar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información la facultad de recabar de los agentes que operan en el sector de las TIC y de la SI en general, la información necesaria para fines estadísticos y analíticos.
- Establecer la obligación de que, a la hora de elaborar los proyectos de obras de construcción de carreteras o de infraestructuras ferroviarias, se prevea la instalación de canalizaciones para el despliegue de redes de comunicaciones electrónicas a lo largo de toda la longitud de las mismas y del equipamiento para asegurar la cobertura de comunicaciones móviles en todo su recorrido.

Modificaciones a la legislación de sociedades

La LISI introduce también algunos cambios respecto a la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada y respecto al texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989. La principal modificación de la legislación de sociedades es la rebaja de manera drástica de los tiempos de constitución de una sociedad limitada, pudiéndose reducir hasta cuatro días. En concreto, la modificación se basa en las siguientes medidas:

1. Introducción de un modelo orientativo de estatutos en la sociedad de responsabilidad limitada.
2. Agilización de los trámites que implican la obtención de una denominación social como paso previo a la constitución de una sociedad de responsabilidad limitada, sin por ello restar importancia a la seguridad que aporta al tráfico mercantil el sistema vigente de denominaciones sociales, tutelado por el Registro Mercantil Central.
2. Facultar a los administradores, desde el otorgamiento de la escritura fundacional, para el desarrollo del objeto social y para la realización de toda clase de actos y contratos relacionados con el mismo.

Preceptos de impulso a la Sociedad de la Información

Por último, la LISI incorpora otros preceptos en su función de facilitador de acceso a la Sociedad de la Información tales como:

- Promover el impulso, el desarrollo y la aplicación de los estándares de accesibilidad para las personas con discapacidad en los diseños y procesos

basados en las nuevas tecnologías de la SI.

- Regular los instrumentos telemáticos necesarios para ser utilizados por aquellos profesionales colegiados que elaboren y preparen proyectos e informes que hayan de incorporarse a los procedimientos que tramiten las Administraciones Públicas.
- Difundir las aplicaciones declaradas de fuente abierta por las propias Administraciones Públicas, así como asesorar sobre los aspectos jurídicos, tecnológicos y metodológicos para la liberación del software y conocimiento.
- Establecer los medios de apoyo y líneas de financiación para el desarrollo de los servicios de la SI promovidos por entidades privadas sin ánimo de lucro.
- Poner a disposición de los ciudadanos, en los términos legalmente establecidos, los contenidos digitales de las Administraciones Públicas de cuyos derechos de propiedad intelectual sean titulares o que pertenezcan al dominio público.
- Ofrecer la posibilidad, tanto a las personas físicas como jurídicas, de poner a disposición del público los contenidos de las obras digitalizadas de las que sean titulares, con la finalidad de fomentar las nuevas tecnologías y la SI entre los ciudadanos.

3. LAS NOVEDADES QUE PROCEDEN DEL MERCADO: MOVILIDAD Y WEB 2.0

3.1. Los nuevos canales de banca a distancia

La mayoría de las entidades financieras españolas ha optado por contar con una red de distribución multicanal que incluye la red de oficinas y distintas modalidades de

banca a distancia, cada una de ellas con características específicas que las hacen idóneas para distintas operaciones o segmentos. Frente al trato personal recibido en las oficinas bancarias, las alternativas de autoservicio, ya sea en cajero, por teléfono o a través de Internet, tienen el valor de la inmediatez y de la disponibilidad permanente, siempre que se cuente con la aceptación por parte de los clientes. Para lograrlo, es necesario proporcionar elementos de control sencillos y, si fuera necesario, incentivar el uso del autoservicio para las operaciones más costosas.

Una de las primeras cuestiones que debe aclararse es el carácter sustitutivo o complementario de cada canal con respecto a los otros y, particularmente, en relación con la red de oficinas bancarias. La banca a distancia es una herramienta poderosa para liberar de la carga de trabajo transaccional a los empleados pero, a día de hoy, casi siempre es necesario complementarla con la red de distribución física, tanto por la importante labor comercial en las oficinas como por la mayor confianza que inspira a los clientes en la contratación de ciertos productos (hipotecas, préstamos personales y, en particular, depósitos, fondos de inversión o seguros financieros). Así pues, la banca a distancia debe considerarse como una oferta de valor añadido a los clientes y como un elemento de fidelización.

La experiencia muestra cómo las entidades españolas con presencia exclusivamente *online* tardaron varios años en asentarse y obtener beneficios en sus primeros años de actividad (2000-2006), coincidiendo con un período de gran crecimiento del sector tradicional¹. Tras un período de adaptación, la evidencia apunta a que la rentabilidad de la banca *online* recae, fundamentalmente, en los depósitos y los créditos hipotecarios², mientras que las entidades

¹ Calvo y Martín de Vidales (2007).

² Fundación Orange (2007), p. 202.

bancarias han asimilado el uso de Internet como un canal adicional para la distribución de una oferta más amplia de productos y servicios.

Uno de los puntos débiles de la banca a distancia es la frialdad de la relación, la falta de cercanía y de comprensión de las necesidades de cada cliente. Por este motivo, el diseño de estos canales debe hacer frente a las reticencias de los usuarios demostrándoles que cada funcionalidad ha sido pensada para ellos. Pese a que se suele hacer hincapié en la seguridad como un factor crítico para los usuarios, algunos estudios de mercado lo sitúan en segundo o tercer lugar en favor de la facilidad de uso y acceso, el verdadero elemento diferencial para los clientes.

La percepción del cliente sobre la tecnología es tan importante o más que las medidas objetivas que se puedan realizar desde las entidades financieras, por lo que la experiencia de usuario ha de pasar a un primer plano estratégico. La sencillez de uso, la disposición lógica de la información y la presentación de mensajes claros y comprensibles mejoran la interacción del cliente bancario con los sistemas de su entidad, mientras que los problemas relacionados con la tecnología producen un alto grado de frustración. En muchos casos, un cliente frustrado renunciará a usar el canal de manera indefinida, y el esfuerzo para recuperarlo será considerablemente mayor que el inicial.

Como cabría esperar, el perfil de los usuarios interesados por los nuevos canales estará íntimamente ligado a la experiencia de usuario que se proporcione. Así, sistemas con cierta complejidad de uso o que requieran un conocimiento previo de la tecnología tendrán mayor aceptación entre la población más joven (acostumbrada a manejar tecnología con soltura) y entre aquella que dispone de un mayor grado de formación académica. Esto se puede ver en el

caso de la banca electrónica en España, que en 2006 era utilizada mayoritariamente por población entre 25 y 44 años (67,1%) y con formación educativa superior (50%)³, en porcentajes muy superiores a los que presentan esos grupos en la pirámide de población española (39,1% y 16,6%, respectivamente).

Tras la sencillez de uso, el segundo factor más apreciado por los usuarios de banca a distancia es la capacidad de personalización, la adaptación de la oferta a las necesidades específicas de cada cliente. Muchas entidades financieras españolas ya ofrecen alertas (por correo electrónico o SMS) relacionadas con movimientos en cuenta o con operaciones de tarjetas de crédito. Algunas incluso adaptan la pantalla de inicio de la banca *online* y de los cajeros automáticos con las operaciones más frecuentes de cada cliente. Sin embargo, todavía se puede ir mucho más lejos si se combinan técnicas de minería de datos (*data mining*) con sistemas de recomendación social y con el estudio de patrones de uso. Algunas operaciones empresariales de los últimos meses, como la entrada de BBVA con 24 millones de dólares en el capital de MyStrands (una empresa española dedicada a la recomendación social de contenidos musicales), muestran un interés creciente de los bancos por conocer mejor los gustos de sus clientes.

El análisis de la información bruta que tienen a su disposición las entidades de crédito, junto con la contratación *online* (que se verá impulsada con la aplicación de la Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información, como se ha visto en el epígrafe anterior) son los siguientes pasos en la creación de servicios mejor orientados al cliente y en el uso de la banca a distancia como canal comercial. La explo-

³ Climent y Momparler (2006).

tación de los datos de clientes debería permitir ofrecer información sobre productos de interés para el cliente y también servicios que puedan ser relevantes para éste, conocidas las operaciones que realiza habitualmente (compra de entradas, domiciliación de recibos...).

El hecho de que las entidades de crédito conozcan cada vez mejor a sus clientes hace surgir también ciertos temores sobre la preservación del derecho a la intimidad y, particularmente, sobre el cumplimiento de la Ley Orgánica de Protección de Datos. Aquí entramos en el terreno de la seguridad y la confianza, que constituye la tercera preocupación de los clientes de banca a distancia. Generalmente, la confianza que transmite la marca de la entidad es suficiente para una mayoría de usuarios, pero la seguridad del servicio ofrecido es esencial para mantener la satisfacción del cliente. Como se verá el apartado posterior dedicado a la seguridad, los sistemas de claves de acceso, la certificación Web y el cifrado de los datos para el envío de información a través de Internet son algunas de las herramientas desplegadas para luchar contra fraudes como el *phishing*, una práctica de suplantación de identidad de empresas que se encuentra en alza y que afecta en un 89% de los casos a empresas de servicios financieros⁴. Previsiblemente, la generalización del uso del DNI electrónico como medio de identificación proporcionará un mayor grado de confianza a los usuarios e impulsará el uso de la banca electrónica en España, que presenta una de las tasas de penetración más bajas de la Unión Europea, con sólo un 31% de los internautas haciendo uso de ella⁵.

3.2. Banca móvil

Dentro de las variantes de banca a distancia, la telefonía móvil, que ha alcanzado niveles de penetración superiores al 100%⁶ en poco más de una década, lleva años evaluándose como herramienta o trampolín para ofrecer servicios financieros. Sin embargo, los intentos de llevar el banco al teléfono móvil en los primeros años 2000 fueron poco exitosos. Entonces, las entidades se toparon con un entorno desfavorable provocado por el estallido de la burbuja 'puntocom' y con una tecnología todavía inmadura para ofrecer servicios atractivos para el público. Los terminales con pequeñas pantallas en escala de grises y las lentas conexiones de datos GSM no proporcionaban una experiencia de usuario satisfactoria y la aceptación fue muy baja, dejando a la banca móvil con una presencia casi testimonial en la distribución multicanal de las grandes entidades.

Unos años después la situación ha cambiado sensiblemente, al menos en lo que a la tecnología se refiere. La extensión de las redes móviles de alta velocidad (UMTS y HSPA) permite ahora la transmisión de datos de manera ágil, y los terminales han evolucionado en consonancia, ofreciendo mayores pantallas en color y capacidades de procesamiento de información que antes sólo estaban reservadas a las agendas electrónicas personales (PDA). Esto ha permitido que se desarrolle una gran variedad de pequeñas aplicaciones que los usuarios pueden descargar a sus teléfonos, desde juegos hasta programas de cartografía pasando, por supuesto, por aplicaciones suministradas por entidades financieras.

Las entidades de crédito tienen a su disposición diversas tecnologías para ofrecer sus productos y servicios empleando teléfo-

⁴ Fundación Orange (2007), p. 39.

⁵ Eurostat (2007).

⁶ Comisión del Mercado de las Telecomunicaciones (2007).

nos móviles. La forma de comunicación más sencilla es la basada en mensajes cortos (SMS), que tienen como principales ventajas su bajo coste, la familiaridad para la mayoría de los usuarios y la compatibilidad con cualquier terminal, sin necesidad de adquirir un modelo de última generación. Este sistema es idóneo para el envío de información a los clientes, ya sea publicidad o, mejor todavía, alertas personalizadas asociadas a la cotización de valores, a los movimientos en cuenta o al uso de tarjetas.

También es posible realizar determinadas transacciones a través de SMS, pero los incentivos para que un usuario utilice este tipo de sistemas en España son limitados. La experiencia de usuario es poco agradable, ya que no se muestra ningún tipo de interfaz gráfica y se debe teclear el código correspondiente para cada operación a realizar, que además varía de una entidad a otra. Frente a esta alternativa, los usuarios suelen preferir desplazarse a una de las más de 38.000 oficinas de bancos, cajas de ahorros o cooperativas de crédito en nuestro país⁷, o bien acceder a la operativa a través de la banca *online*. En España, HalCash fue uno de los primeros servicios financieros en usar esta tecnología. Esta iniciativa, promovida por un grupo de bancos y cajas de ahorros españoles, a los que se unió el Banco de Guayaquil (Ecuador), permite el envío de fondos a un usuario de teléfono móvil, que puede retirar el efectivo en los cajeros automáticos de las entidades adscritas introduciendo un código recibido por SMS. Aunque estos servicios no gozan de éxito masivo en España, en países con menores niveles de bancarización, la alta penetración del teléfono móvil lo convierte en un canal relevante de distribución de servicios financieros, como demuestra el éxito

de soluciones como M-PESA (Kenia), Wizzit (Sudáfrica) o G-Cash (Filipinas).

El siguiente avance conceptual en la prestación de servicios financieros en movilidad es el acceso a un portal de banca electrónica adaptado a los dispositivos móviles. En esencia, el cliente navega por una versión reducida (WAP), tanto en tamaño como en funcionalidades, del canal de banca *online*. El principal inconveniente de esta modalidad de acceso es la usabilidad, marcada negativamente por la lentitud de las conexiones y por el escaso atractivo de la interfaz de usuario; además, los operadores de telecomunicaciones móviles suelen ofrecer tarifas de datos poco comprensibles y significativamente más caras que sus equivalentes fijos. En los próximos meses, la evolución de los terminales móviles y de los planes de precios ofrecidos por los operadores podría cambiar este escenario. Un buen ejemplo próximo a desembarcar en España es el iPhone, el novedoso teléfono de Apple, que incluye un navegador Web completo y que ha sido comercializado en exclusiva en varios países junto con una tarifa plana de datos.

Otra modalidad de banca móvil que soluciona algunos de los inconvenientes del acceso WAP es la instalación por parte del usuario de una pequeña aplicación (generalmente programada en lenguaje JAVA) suministrada por la entidad financiera. En este caso, el acceso a la información y a la operativa bancaria es más atractivo para el cliente, ya que la presentación de la información se hace de manera similar a como se lleva a cabo en cualquier otra herramienta del teléfono. En contrapartida, exige un terminal más sofisticado y el cliente debe ser capaz de instalar el software, algo para lo que no está capacitada una mayoría de clientes.

Son muchas las entidades financieras españolas que ofrecen los servicios de banca móvil ya descritos. No obstante, su

⁷ Asociación Española de Banca (2007) y Confederación Española de Cajas de Ahorros (2007).

relevancia cuantitativa sigue siendo limitada en el contexto de la estrategia multicanal, por las complicaciones que plantea la tecnología, por el alto coste de las conexiones de datos para los usuarios o por la existencia de alternativas más cómodas y atractivas (como la banca *online*). Pese a esto, algunas entidades están haciendo apuestas estratégicas por este canal. Entre ellas, Bankinter anunció en diciembre que se convertiría en la primera entidad financiera española que comercializaría con su propia marca tarjetas de telefonía móvil (SIM) habilitadas para realizar operaciones de banca electrónica. Para poder ofrecer este nuevo servicio, el banco ha firmado un acuerdo con el operador holandés KPN, como ya hiciera un año antes Rabobank en su mercado doméstico. Además de la operativa bancaria habitual, la integración de las aplicaciones financieras en las SIM permite dotar de mayor seguridad a las operaciones, puesto que se incluye un módulo de cifrado de datos.

No obstante, es relevante poner de manifiesto que las mayores tasas de crecimiento de clientes activos en banca a distancia se están produciendo en los servicios de banca móvil por encima del crecimiento de los usuarios de la banca por Internet tradicional o la propia oficina física.

A medio plazo, es previsible que el uso del móvil como medio de acceso a servicios financieros en España adquiera nuevas vertientes, como ya se observa en mercados internacionales. Una de ellas es la integración de tarjetasmonedero equipadas con tecnologías inalámbricas (como PayPass, de Mastercard, o PayWave, de Visa), que está llamada a facilitar las pequeñas compras sin necesidad de emplear efectivo. A partir de ahí, cabe esperar que las siguientes innovaciones en banca móvil estén relacionadas con la tendencia hacia las redes sociales y la participación activa de los

clientes, como ya se observa en el canal de banca *online*.

3.3. Innovación en los servicios financieros en Internet

En los últimos años se ha generalizado el uso de la expresión Web 2.0 para referirse a un nuevo paradigma de Internet, más centrado en el usuario: sus gustos, sus intereses, el contenido que es capaz de generar, sus interacciones con otros usuarios... De hecho, la revista Time eligió como persona del año 2006 al genérico «Tú» («You») como reflejo de la relevancia adquirida por las redes sociales y las páginas dedicadas a la exposición de contenidos creados por los usuarios. Ese mismo año, la empresa Google, dedicada a la búsqueda automática de contenidos en Internet, cerraba la compra de YouTube, una página donde los usuarios pueden subir sus propios videos, por 1.600 millones de dólares; apenas había pasado un año desde su fundación.

Las entidades financieras deben saber adaptarse a este nuevo entorno de mayor poder para los clientes, y eso implica entender Internet como un medio con sus propias condiciones de comunicación con el mercado. Cuestiones como la transparencia en la gestión, la personalización de los servicios o la comunicación bidireccional deben ser el objetivo de esta nueva estrategia, puesto que la mayoría de los internautas comparan ahora la oferta de diversas entidades antes de tomar una decisión de contratación de productos financieros⁸. Por lo tanto, las entidades de crédito deberán acompañar a sus clientes en todo el proceso comercial a través de Internet para lograr su mayor satisfacción: conciencia de una necesidad; búsqueda de ofertas; comparación y selección; adquisición; búsqueda de servicios asociados.

⁸ Heng, Meyer y Stobbe (2007).

Los bancos, cajas de ahorros y cooperativas de crédito españolas no son del todo ajenos a estos cambios y hace tiempo que permiten a sus clientes personalizar ciertos aspectos como las pantallas de acceso a la banca electrónica y la configuración de alertas. Algunos, incluso, disponen de *blogs* corporativos y fuentes de noticias como medio de acercarse más a sus clientes. Los más aplicados ya han trasladado estos nuevos conceptos a su propia organización y favorecen la participación de sus empleados poniendo a su disposición herramientas de trabajo colaborativo que mejoren los flujos de información interna.

Este tipo de innovación, que podríamos denominar disruptiva por los cambios radicales introducidos sobre la visión y la cultura empresarial, se basa en el conocimiento profundo de la propia organización y del cliente. Por un lado, las ventajas de introducir cambios organizativos de este tipo influyen positivamente sobre el posicionamiento de la entidad como empresa innovadora, sobre la implicación de los empleados en los procesos de decisión y sobre su satisfacción por el reconocimiento mostrado hacia ellos. Por el otro, el conocimiento del cliente y de sus necesidades, sin necesidad de que éste las manifieste explícitamente (mediante el análisis de sus relaciones y sus hábitos) hace más efectiva la labor comercial y lo fideliza para la entidad. En este sentido, Internet ha abierto las puertas a otras formas de prestar servicios financieros a particulares. El concepto de red social se ha aplicado a la creación de nuevos sistemas de préstamos y a la gestión de las finanzas personales, entre otros.

Los préstamos P2P o usuario-a-usuario aprovechan Internet para conectar la oferta y la demanda de crédito entre desconocidos. Plataformas como Zopa en el Reino Unido o Prosper en Estados Unidos ya han puesto en marcha esta idea, desarrollando al mismo tiempo sistemas de calificación

crediticia y de diversificación de riesgos para proporcionar la mayor confianza posible a las partes. Algunas variantes de este tipo de iniciativas están orientadas a la financiación de proyectos empresariales por parte de internautas que forman grupos de inversores, como ocurre en Frooble (Holanda) o en Partizipa (España); y otras páginas se han especializado en la concesión de pequeños préstamos a emprendedores en países en desarrollo. Kiva y Microplace (este último promovido por la empresa estadounidense eBay) son dos buenos ejemplos de sitios dedicados a microfinanzas.

Otra innovación que está gozando de un éxito relativo (aún es pequeño si lo comparamos con el número de usuarios de banca *online*, por ejemplo), especialmente en Estados Unidos, son los sitios dedicados a la gestión de finanzas personales. Existen multitud de empresas como Buxfer, Wesa-be o Mint en las que los usuarios pueden llevar un control de sus cuentas bancarias, además de intercambiar consejos de ahorro e inversión con otros usuarios e, incluso, comparar su balance financiero personal con el de otros usuarios con los que compartan parámetros como el sector de actividad, la categoría profesional, la edad o la ubicación geográfica. En España, Money-trackin' ofrece algunas de estas funcionalidades, además de un localizador geográfico (asociado a un mapa proporcionado por Google) de ofertas de ahorro.

Estos nuevos servicios cubren pequeños nichos de mercado que no afectan al negocio de las entidades financieras, aunque no hay que olvidar que la innovación provoca que la oferta de productos y servicios se amplíe. Por este motivo, los bancos y cajas deben vigilar las tendencias para mantener su posición de liderazgo en el mercado. En este sentido, las empresas más innovadoras podrán suministrar soluciones que se integren en los canales de banca a distan-

cia del sector financiero, aportando una ventaja comparativa frente a la competencia.

4. LAS NOVEDADES FRUTO DE LA EVOLUCIÓN DE LAS FUNCIONALIDADES DE LA BANCA ONLINE: ¿CÓMO MEJORAR LA EXPERIENCIA DE USUARIO?

4.1. Evolución de la banca online en España

La evolución de la banca *online* en España no ha sido uniforme. Los bancos, especialmente los puramente *online* (sin red de oficinas) y algunas entidades que apostaron fuerte por el nuevo canal desde el primer momento, lideraron en un principio los avances, aunque el estallido de la burbuja tecnológica del 2001 supuso un freno para el conjunto del sector. El resto de los bancos, cajas de ahorros y cooperativas de crédito fueron mas lentos en la implantación de la banca *online* pero, especialmente a partir de 2004, las distancias se fueron acortando y la apuesta por la banca *online* se generalizó. En este sentido, se pueden distinguir tres fases diferenciadas, como se ha podido observar en el informe de *benchmarking* de banca *online* elaborado por Afi⁹:

—Primera fase (hasta 2002). En este primer momento el mercado mantiene una oferta centrada fundamentalmente en las posibilidades de consulta de los productos que el consumidor tiene contratados. Sin embargo, la información disponible, era, por regla general, de peor calidad que la que podría obtener un cliente dentro de los canales tradicionales, ya que no ofrecía un suficiente nivel de detalles específicos. A esto había que añadir que este canal, mucho menos personal que el

resto, carecía de unos buenos medios de asesoramiento sobre productos que pueden ser poco conocidos por muchos de los potenciales usuarios de la banca *online*. Además, las plataformas de contratación y la gama de productos contratables a través de la Red, específicos o no de este canal, estaban poco desarrollados. De esta manera, el servicio al que tenía acceso un hipotético cliente virtual de aquel periodo era, en su conjunto, de peor calidad que el que ofrecía la entidad a través de sus canales tradicionales. Durante esta fase numerosas entidades mantuvieron páginas meramente informativas, poco más que escaparates virtuales.

En esta fase tuvieron un papel particularmente relevante los servicios centralizados de soporte tecnológico que comenzaron a prestar servicios a determinadas cajas de ahorros y cooperativas de crédito. En este grupo se incluyen Rural Servicios Informáticos (RSI), Infocaja, Infodesa, la Confederación Española de Cajas de Ahorros (CECA), Asociación Técnica de Cajas de Ahorros (ATCA) y Ahorro Corporación.

—Segunda fase (hasta 2004). Las entidades líderes centraron sus esfuerzos en mejorar la operatividad y en un incremento de la gama de productos contratables y las posibilidades de consulta ofrecidas a los clientes sobre los productos que éstos ya tenían contratados en la entidad. En esta etapa se observa un incipiente avance realizado por determinadas cajas de ahorros y cooperativas de crédito. No obstante, el grueso de las cajas aún se mantiene relativamente retrasado frente a los bancos, aunque algunas entidades comenzaron a ocupar posiciones de liderazgo.

⁹ Afi-net Global (2002-2007).

—Tercera fase (a partir de 2004). Las entidades puramente *online* comenzaron a obtener beneficios, lo que supuso el fin de las especulaciones sobre la viabilidad del canal *online* y enterró definitivamente el estancamiento que había resultado de la crisis del 2001. Las cajas de ahorros en su conjunto mostraron un claro interés por el desarrollo de sus portales de banca electrónica, especialmente destacado en entidades que hasta entonces habían permanecido en un segundo plano.

4.2. Tendencias actuales

Entre las tendencias que se observan en el sector destaca la acelerada desaparición de los modelos de banca *online* carentes de capacidades transaccionales y, por tanto, con un carácter fuertemente presencial. Actualmente encontramos en el mercado tan solo entidades englobadas en el modelo mixto (presencial y *online* y, en menor medida, en el modelo puramente virtual (cabe destacar que algunas entidades que nacieron como puramente virtuales han evolucionado hacia modelos mixtos).

A partir del 2005 se ha percibido un considerable avance en los desarrollos acometidos por el conjunto de la banca electrónica en España. Sin duda, los favorables resultados económicos obtenidos por las entidades puramente *online* han contribuido a acelerar este impulso. Una parte significativa del esfuerzo se ha dedicado a renovar sustancialmente el diseño gráfico de las páginas. Los cambios en diseño obedecen en parte al abandono del modelo de escarinate, pero más relevante ha sido el creciente interés, por parte del sector en su conjunto, por la usabilidad. Los portales con mala disposición de elementos funcionales y diseños gráficos poco afortunados han dado paso a páginas mucho más livianas y, por tanto, más rápidas de cargar, en las que la organización de la información ha

cobrado una importancia central, algo imprescindible para facilitar la navegación por un creciente número de productos y servicios.

La mejora en la calidad de las conexiones a Internet, con la implantación cada vez más generalizada de la banda ancha, ha permitido una mayor libertad en el diseño gráfico, hasta muy recientemente encostrado por la necesidad de una carga rápida de las páginas. El incremento en la potencia de los procesadores y el abaratamiento de la memoria también han redundado en mejores prestaciones de las aplicaciones de banca *online*, lo que ha tenido un efecto positivo en la aceptación por parte de los usuarios.

Otro de los factores que está impulsando la mejora de los portales es la experiencia acumulada por el sector. Esta experiencia ha permitido que las entidades presten una mayor atención a aspectos que en las primeras fases de desarrollo quedaban frecuentemente descuidados. Por ejemplo, la abundancia de plataformas y portales diferenciados dificultaba la navegación, al tiempo que incrementaba los costes de mantenimiento del servicio. A lo largo de los últimos años se observa una clara tendencia a la integración, buscando una mayor efectividad y una reducción de los costes. Sin embargo, muchas entidades mantienen y potencian los portales diferenciados en casos considerados estratégicos, como los portales de empresa o los destinados a los jóvenes.

Cabe destacar cómo las entidades están trasladando con creciente agilidad a la Red los productos que ofrecen un mayor interés comercial. Los cambios en la legislación tributaria, por ejemplo, impulsaron en su momento el auge de los planes de pensiones y el declive de los *unit linked*, y más recientemente hemos podido ver la rapidez con la que aparecían en las Webs de las entidades punteras nuevos productos

como los planes individuales de ahorro sistemático (PIAS). Esta tendencia se enmarca dentro de una estrategia de adecuación de las Webs a la comercialización de los productos. Las mejoras en tecnología han permitido dar una mayor flexibilidad y una gestión más sencilla de las páginas. De esta forma, las entidades pueden realizar ajustes a la oferta respondiendo más velozmente a la información que se va recogiendo y a los cambios de estrategia.

La adecuación del servicio a los fines comerciales de las entidades influye también en la organización y estructura de los contenidos. Por ejemplo, las herramientas de asesoramiento y formación, antes concentradas en secciones específicas, se integran de forma creciente con los productos relacionados, siempre buscando un mayor apoyo a las ventas y el cumplimiento con la normativa. Los nuevos diseños permiten a su vez destacar los productos, que ofrecen un mayor interés en cada momento. Por otro lado, es previsible que las entidades sigan incrementando la oferta de productos que se ajusten a las características particulares de cada cliente individual. Los avances en las técnicas de minería de datos y el volumen de información disponible sobre cada cliente ya lo hacen posible, pero tan solo una minoría de las entidades ha implementado esta estrategia.

Sin embargo, este proceso de expansión de la oferta entraña ciertos riesgos, pues algunos productos antes reservados a una minoría de clientes, como los *warrants*, pueden ser contratados por individuos que no los conocen lo suficientemente. Los requisitos de información y las limitaciones de oferta exigidas por la legislación vigente (especialmente la Directiva MiFID), corrigen estos problemas en algunos casos, pero corresponde a las entidades financieras asegurarse de que el canal *online* ofrece un grado de formación y asesoramiento al menos equivalente al que se ofrece en las

oficinas. Las herramientas de asesoramiento y formación vinculadas directamente a los productos ofertados permiten cumplir estos requisitos.

En este contexto, las nuevas tecnologías, como AJAX, han permitido incorporar de forma mucho más simple herramientas sumamente complejas que permiten realizar simulaciones interactivas ajustadas a productos concretos. La amplia oferta de hipotecas, especialmente en los años 2006 y 2007, tuvo su reflejo en simuladores que suministraban informes con las condiciones precisas de cada una de ellas, así como sus ventajas. Los *brokers online* también han experimentado un impulso significativo, gracias a la mayor interactividad, con una mejor selección de la información suministrada a los inversores.

Algunas iniciativas novedosas rompen la separación estricta entre canales. Por ejemplo, Bankinter ha lanzado un servicio de atención por videoconferencia accesible desde su página Web. ¿Se trata de atención telefónica o de un servicio *online*? Sin duda una combinación entre ambas, con un amplio potencial futuro, y que puede mejorar significativamente la experiencia, especialmente de usuarios reacios a acercarse al servicio *online* pero que pueden encontrar en el mismo una referencia conocida y un punto de apoyo humano que facilite la transición hacia el nuevo canal.

Las entidades están intentando acercarse a los clientes implantando las tecnológicas Web 2.0 examinadas anteriormente. La distribución de *widgets*, o pequeños programas que el usuario instala en su escritorio de PC y que proveen información actualizada (cotizaciones de bolsa, alertas de operativa en cuenta, etc.), constituye un buen ejemplo, como lo es la distribución de boletines de noticias (*newsletters*) informativos.

5. LAS NOVEDADES QUE SURGEN DEL ÁMBITO DE LA SEGURIDAD: INICIATIVAS PARA IDENTIFICAR A LOS USUARIOS E INICIATIVAS PARA DEFENDERSE DE LOS ATAQUES

5.1. ¿Es segura la banca online?

Uno de los más importantes retos a los que se sigue enfrentando la banca a distancia es la seguridad. Este problema tiene una doble vertiente: por un lado, supone un riesgo económico directo tanto para los clientes como para las entidades, pero además hay que añadir que el temor al fraude constituye un freno considerable a la expansión del canal, ya que un número significativo de usuarios lo rechaza debido a la elevada percepción de inseguridad detectada en el público general.

El reforzamiento de las medidas de seguridad llevado a cabo por los servicios informáticos, incluyendo el cifrado de los datos y la vigilancia exhaustiva de los sistemas de defensa para evitar ataques, han hecho extraordinariamente difícil la realización de ataques exitosos contra las entidades bancarias. Sin embargo, los clientes tienen un grado muchísimo mayor de indefensión, derivado de su desconocimiento del medio así como de la vulnerabilidad de los equipos informáticos domésticos.

Los datos son, desde luego, preocupantes. Según un estudio del Instituto Nacional de Tecnologías de la Comunicación (INTECO)¹⁰, basado en encuestas realizadas a usuarios en todo el territorio nacional en 2007, el número de personas afectadas por algún tipo de fraude relacionado con la banca por Internet ha superado los 300.000. El número que declara haber sufrido pérdidas económicas es muy inferior,

apenas un 2,1%, pero la media de las pérdidas fue de 539 euros.

Otro estudio publicado recientemente por la empresa RSA Security¹¹, indica que España se ha convertido en el tercer país del mundo con un mayor número de intentos de fraude relacionados con la banca online, con un 7% del total mundial. El número de ataques globales se ha mantenido relativamente constante a lo largo del 2007, según un informe del Anti Phishing Working Group (APWG)¹², que registró un pico de cerca de 39.000 ataques registrados en septiembre, seguido de un descenso gradual hasta los 25.700 ataques registrados en diciembre. Según esta organización, la banca acumula el 91,7% de todos los ataques detectados en el mes de diciembre de 2007.

Una característica singular de este tipo de fraude es que, debido a su propia naturaleza (facilidad relativa del lanzamiento del ataque, reducido periodo de reacción entre el inicio del mismo y la capacidad de las entidades, falta de prevención por parte de los usuarios finales), hace que detrás de los mismos se pueda encontrar tanto grupos altamente sofisticados como pequeñas operaciones organizadas por un grupo reducido de individuos que solo pretenden obtener cantidades relativamente pequeñas de dinero. Los medios de comunicación anuncian con cierta regularidad la captura de responsables de redes dedicadas a este tipo de fraudes con estafas que alcanzan cantidades que van desde los pocos miles de euros hasta los varios millones. Este mes de febrero se anunció el desmantelamiento en España de una red compuesta por 76 individuos que habían logrado un botín de tres millones de euros.

¹⁰ Instituto Nacional de Tecnologías de la Comunicación (2008).

¹¹ RSA Security (2008).

¹² Anti Phishing Working Group (2008).

El propio Banco de España declaró en su Memoria de Reclamaciones¹³ presentadas en septiembre del 2007 que los «intentos de fraude por Internet han crecido de formas alarmante en los últimos tres años». Según el regulador, el número de ataques de *phishing* pasaron de 33 en el 2004 a 1.184 en el 2006, último año para el que han publicado datos.

Aunque el sector se reserva los datos reales de fraude por Internet, de los estudios anteriores podemos deducir que la situación tiene un alcance significativo y potencialmente dañino para el crecimiento del sector. Cabe insistir en que el elemento más vulnerable de la cadena lo constituye el usuario final, por lo que facilitar la mayor cantidad posible de información al mismo constituye una de las formas más efectivas de atajar el problema.

En este contexto, este artículo explorará en primer lugar las formas de identificación utilizadas por el sector en la actualidad, y que constituyen la primera y más importante barrera contra el fraude. A continuación se explorarán las principales formas de fraude utilizadas, especialmente los mecanismos que permiten la apropiación de claves de acceso. En tercer lugar se examinarán las medidas tomadas por las entidades financieras para defenderse a sí mismas y para defender a los usuarios, así como las precauciones que éstos deberán tomar para minimizar la posibilidad de fraudes. Finalmente comentaremos el papel que los organismos reguladores pueden jugar para contribuir a la resolución del problema.

5.2. Formas de identificación

La cuestión central en todas las transacciones que se realizan por Internet, inclu-

yendo las transacciones de banca electrónica, radica en que las partes involucradas en dichas transacciones tengan la seguridad de que la parte con la que están tratando sea efectivamente la que esperan. Como veremos en el siguiente epígrafe, la mayor parte de los fraudes cometidos se basan en defraudar dicha confianza, presentándose los defraudadores como una entidad legítima ante los clientes, o como clientes legítimos ante una entidad bancaria.

La totalidad de las entidades financieras españolas exige a los usuarios una clave de usuario y una contraseña para acceder a la zona privada de la banca *online*. Por lo general, esta clave y esta contraseña suelen ser estáticas (no cambian con el tiempo) pero algunas entidades sí exigen renovaciones periódicas o la utilización de diferentes mecanismos de coordenadas, que hacen que el usuario o la clave (generalmente esta última) varíen en cada acceso. Es habitual que, si se intenta el acceso de forma incorrecta en más de tres ocasiones, la cuenta quede bloqueada y sea necesario acudir a la entidad para desbloquearla. Una vez superado este primer mecanismo de identificación, los usuarios pueden realizar consultas, pero no operaciones.

Para poder realizar operaciones es necesario efectuar un segundo nivel de validación, o firma, que tiene un nivel más elevado de seguridad. Por lo general esta firma se exige en cada operación que el usuario desee realizar. Para la firma las entidades no suelen utilizar una contraseña estática, sino que utilizan diversos mecanismos de generación dinámica de claves. Los más habituales son la tarjeta de coordenadas, los *tokens* (*hardware* virtual) o pequeños dispositivos que generan contraseñas de forma automática, tarjetas USB, o el envío de la contraseña mediante SMS al móvil.

La combinación de una primera identificación y de una firma adicional para operaciones, si se hace de forma correcta, supo-

¹³ Banco de España (2007).

ne una garantía suficiente, aunque no infalible, de que la persona realizando la transacción es realmente el usuario autorizado.

La implantación del Documento Nacional de Identidad electrónico (DNle) ha supuesto un paso adicional a la hora de garantizar la identificación del usuario. En la actualidad tres entidades financieras ya lo aceptaban en sus servicios de banca *online*: Caixa Galicia, Bankinter, Caja Madrid y Kutxa Gipuzkoa Donostia. Aunque el mecanismo puede variar según la entidad, el usuario tiene que introducir el DNle en el lector correspondiente (cuyo coste de adquisición es muy bajo). Este lector verifica la información contenida en el microchip cifrado del DNle. En la primera ocasión deberá introducir además su clave de acceso habitual y su firma adicional. A partir de ese momento, bastará con introducir su DNle en el lector y el PIN correspondiente tanto para poder acceder como para poder realizar transacciones. Todas las entidades permiten la identificación tanto mediante el DNle como mediante las técnicas tradicionales.

EL DNle, en cuya implantación España es un país pionero a nivel mundial, resuelve el problema de la multiplicidad de claves de acceso y de mecanismos de firma a la que se enfrentan los usuarios de Internet. Una vez que sea plenamente aceptado por el sector privado (ya lo es en la administración pública) bastará con disponer del DNle y su PIN para poder confirmar de forma fehaciente su identidad y de esta forma realizar todo tipo de transacciones sin la necesidad de memorizar numerosas claves o de portar distintas tarjetas de coordenadas, dispositivos *token*, etc.

5.3. Ataques más frecuentes en la banca online

Las entidades financieras tienen una larga experiencia en la detección y en la lucha contra el fraude. El sector ha sido líder

en innovaciones tecnológicas en este campo y sus sistemas internos se consideran suficientemente seguros. Sin embargo, los sistemas utilizados por los clientes finales para acceder a la banca *online* gozan de una seguridad incomparablemente menor, a lo que se suma el bajo nivel de conocimiento tecnológico de la mayor parte de estos usuarios. Por estas razones, los ataques más habituales contra los servicios de banca a distancia se basan en modelos de lo que se conoce como ingeniería social, es decir, la manipulación de los usuarios con el fin de obtener de forma fraudulenta sus datos confidenciales, que se emplearán para obtener beneficios económicos suplantando su personalidad. A menudo, la ingeniería social se ve complementada con subterfugios de carácter tecnológico que incrementan la efectividad del ataque.

El ataque más frecuente es también el más simple: solicitar directamente a los clientes que faciliten, mediante cualquier pretexto, su usuario y su contraseña. A este ataque se le conoce como *phishing* y el método más frecuente utilizado es el envío masivo de correos electrónicos que aparentemente vienen de una entidad financiera. En ocasiones, estos correos son sumamente burdos y generan de forma inmediata la alerta de los receptores, pero en otras ocasiones pueden ser mucho más sofisticados y difíciles de detectar. En algunos casos van personalizados y se dirigen a clientes reales de las entidades atacadas. A los correos electrónicos se han sumado recientemente el envío de cartas postales y de correos SMS. Según el informe de APWG, a nivel mundial solo en el mes de diciembre pasado 144 entidades financieras fueron atacadas mediante este sistema, y en dichos ataques se emplearon un total de 25.000 direcciones Web (URL) fraudulentas con el fin de obtener los datos confidenciales.

Estos ataques son rápidamente detectados por las entidades que, conjuntamente

con las autoridades, son capaces de neutralizarlos, en la mayoría de las ocasiones, en menos de 48 horas; pero aún así se estima que aproximadamente un 1% de los receptores del *phishing* revelan a los atacantes su identidad y su contraseña (aunque eso no suele ser suficiente para que puedan completar el fraude, como veremos más adelante). Según el Banco de España, en los últimos tres años se ha podido enviar más de 700 millones de correos destinados a la práctica del *phishing*, aunque una gran parte de ellos ya son filtrados y eliminados por sistemas automáticos de seguridad en el correo y nunca llegan a sus destinatarios.

En la mayoría de estos correos se invita al usuario desprevenido a conectarse a una página Web de aspecto muy similar a la página habitual de su entidad financiera, para que se identifique. Esta página Web está controlada por los delincuentes y con ella obtienen los datos necesarios para cometer fraudes en el futuro. En los casos mas sofisticados, esta páginas redirigen al usuario hacia las páginas legítimas de la entidad con lo que nunca llega a percatarse del engaño.

El segundo ataque más frecuente es la instalación de *spyware*, o programas espía, que registran los movimientos de los teclados y captan la información sensible que luego envían a servidores controlados por los delincuentes. Este tipo de ataques se ve favorecido por la existencia de incontables ordenadores personales que no cuentan con la necesaria protección contra este tipo de infecciones. Según el informe de APWG, en diciembre de 2007 se detectaron 269 aplicaciones, o virus activos, de este tipo, que en sus diferentes mutaciones utilizaban hasta 2.260 URLs distintas para enviar los datos robados a los clientes. Los cambios de URL se realizan porque, al ser descubiertos los ataques y neutralizadas las URLs utilizadas en los mismos, se ponen en funcionamiento nuevas URLs que permiten continuar con el fraude. Este tipo de ata-

ques se suelen denominar como *pharming*, y se diferencian del *phishing* en que en el primer de los casos el usuario entrega voluntariamente, aunque bajo engaño, sus datos de acceso ante una petición fraudulenta, mientras que en el segundo caso un software fraudulento captura los datos personales, sin que el usuario sea conciente de ello, mientras accede de forma habitual a una cuenta legítima de su institución.

Un tercer tipo de ataque consiste en la apropiación de una sesión legítima mediante la utilización de técnicas conocidas como *Cross Site Scripting* o Inyección de Código. La responsabilidad de luchar contra ellos recae fundamentalmente sobre las entidades financieras, y no sobre los usuarios finales, por lo que el riesgo que comportan es, en términos generales, menor.

5.4. Lucha contra el fraude: el papel de las entidades y de los usuarios

A pesar de la escala de los ataques a los que se somete la banca *online*, el sector fue en sus inicios relativamente lento en la implantación de las medidas de seguridad necesarias no solo para evitar los fraudes sino también para generar confianza entre los clientes. La reticencia que han mostrado por lo general las entidades bancarias se debe a los costes asociados con la implementación de los mecanismos de doble identificación. En España el método más utilizado es la tarjeta de coordenadas, un sistema más barato que los basados en hardware (tarjetas, dispositivos USB, lectores biométricos) y que no se ve penalizado por la relativamente escasa aceptación de la firma digital mediante combinación de claves públicas y privadas. La implantación del DNle como forma de identificación segura supone un decisivo avance en la lucha contra el fraude.

A partir del año 2005 la aparición de informaciones alarmantes en prensa sirvió como impulso para que el sector en su con-

junto incrementara las medidas de seguridad y, muy especialmente, dedicara una atención considerable a suministrar la información necesaria al respecto a sus clientes. A lo largo del 2005 y del 2006 la mayor parte de las páginas Web de las entidades financieras incorporaron llamativos anuncios de seguridad y una sección completa, accesible desde la portada, con amplia información sobre cómo evitar el fraude. También fue habitual el envío de cartas por vía postal en las que se incluían advertencias y explicaciones. En la actualidad se siguen incluyendo advertencias tanto en la correspondencia postal como en la electrónica, así como en las propias páginas Web.

Sin embargo, más allá de la doble identificación y de los esfuerzos por mejorar el nivel de conocimiento de los clientes, las entidades tendrán que hacer un esfuerzo a la hora de establecer mecanismos de seguimiento, en múltiples niveles, de la actividad de sus clientes, para detectar de forma activa posibles fraudes. El análisis de patrones de comportamiento, y el seguimiento de otros aspectos, como la geolocalización del usuario basada en la dirección IP desde la que se conecta, pueden servir para detectar a tiempo acciones sospechosas.

Además, aunque el conjunto de las entidades han adoptado el protocolo de cifrado SSL de 128 bits, mucho más robusto que la versión anterior, por razones de velocidad de carga, un número elevado de entidades no incluye este protocolo de cifrado en la página de inicio, sino solamente en las páginas transaccionales. Esto puede suponer un cierto riesgo, derivado de la incertidumbre que se puede producir a la hora de distinguir páginas legítimas frente a páginas fraudulentas creadas por delincuentes.

Finalmente, otra de las medidas de seguridad adoptadas fue la introducción de claves y firmas mediante teclados virtuales (en los que la posición de las letras y números

varía de forma aleatoria) para imposibilitar los ataques de *pharming*.

Sin embargo, el punto más débil de la cadena de seguridad siguen siendo los usuarios. Corresponde a éstos tomar conciencia de la importancia de adoptar las medidas de seguridad necesarias para minimizar el fraude. Para ello deben tomar las siguientes medidas:

1. Instalar programas antivirus y antimalware en sus ordenadores.
2. Jamás responder a una petición de claves o usuarios recibida por correo electrónico o por cualquier otro medio.
3. Extremar las precauciones si se está utilizando un ordenador público.
4. No acceder a las páginas Web de las entidades financieras pulsando en enlaces encontrados en correos electrónicos o en páginas Web desconocidas: teclear siempre manualmente la URL de la entidad.
5. Confirmar que la transacción utiliza el protocolo seguro (la URL del navegador debe empezar por «https»).
6. Asegurarse de que, una vez finalizada la transacción, el usuario se desconecta completamente de la entidad, preferiblemente cerrando el navegador.
7. Contratar los servicios de alerta disponibles en su entidad, siendo uno de los más efectivos el envío de mensajes SMS cada vez que se produce una transacción. Si bien, este servicio no suele ser gratuito y, por tanto, supone un coste de seguridad que se repercute al cliente.

5.5. El papel de los bancos centrales en la lucha contra el fraude

El alcance del fraude observado, así como la intensidad y creciente sofisticación de los ataques, hace necesario que

las autoridades reguladoras fijen un marco mínimo de seguridad que venza las posibles reticencias de las entidades a adoptar medidas que pueden ser costosas o complejas. En el año 2006 la Autoridad Monetaria de Hong Kong tuvo la iniciativa pionera de adoptar el sistema de doble identificación, con un dispositivo específico, para todas las entidades de banca *online* sujetas a su supervisión.

En esa época, el Federal Financial Institutions Examinations Council (FFIEC), una organización paraguas que engloba los reguladores estadounidenses de la banca, publicó una nueva guía sobre los mecanismos de seguridad que deben adoptar las entidades bancarias norteamericanas¹⁴. Esta guía pone especial énfasis en la adopción de sistemas de doble identificación, algo que cobra especial relevancia ya que el coste adicional que estos mecanismos pueden suponer, siempre se ha considerado un freno para su puesta en marcha, especialmente en los Estados Unidos. Si bien las guías del FFIEC no se pueden considerar como regulación propiamente dicha, a partir del final del 2006 el grado de cumplimiento de las recomendaciones contenidas en las mismas comenzaron a ser utilizadas por las organizaciones reguladoras a la hora de evaluar las prácticas bancarias de las entidades que supervisan, por lo que sin duda tendrán un considerable impacto.

Entre los objetivos que se citan en la guía se incluyen, además de la protección de los datos de los clientes legítimos y la lucha contra el fraude, la prevención de lavado de dinero y de la financiación de los grupos terroristas. La guía no recomienda una tecnología específica de doble identificación, pero exige que cada entidad realice un análisis de las necesidades de seguridad para cada producto o servicio que ofrece en la

Red. Además, se requiere que las entidades evalúen las posibles acciones para mitigar los posibles riesgos de seguridad, y que midan y evalúen el nivel de conocimiento que los clientes tienen tanto sobre los riesgos como sobre las medidas adoptadas para prevenirlos. La tecnología a adoptar dependerá del resultado de estos análisis.

En nuestro país no todas las entidades disponen de estos mecanismos, a pesar de la intensidad de los ataques que se vienen registrando, especialmente de *phishing*. Sería conveniente que se exigiera al conjunto de las entidades de nuestro país que cumplieran, al menos, recomendaciones similares a las que se verán sujetas el año que viene las entidades estadounidenses. El Banco de España se ha limitado por el momento a alertar a las entidades de la necesidad de tomar las medidas adecuadas, pero sin dictar medidas concretas. En febrero del 2007, sin embargo, el Banco de España frenó una aspiración de las entidades financieras de hacer recaer sobre los clientes toda la responsabilidad en los casos de banca a distancia. El Banco de España adoptó este criterio considerando que los clientes frecuentemente utilizan este canal impulsados por la propia entidad, y que en ocasiones son víctimas del fraude pese a haber tomado todas las precauciones razonables. Esta decisión del Banco de España correctamente transmite la presión necesaria a las entidades financieras, pero si el número de reclamaciones por fraudes de este tipo continúa incrementándose, tal vez sea necesaria la adopción de medidas adicionales destinadas a garantizar la seguridad de los clientes.

6. CONCLUSIONES

El papel extraordinariamente relevante de los servicios bancarios en la economía española está relacionado, sin duda, con la notable contribución del sector al desarrollo de la SI. No obstante, el avance en términos

¹⁴ Federal Financial Institutions Examination Council (2005).

de innovación y penetración de los servicios bancarios a distancia ha sido posible en gran medida gracias a la evolución del entorno regulatorio (promovida por la Administración Pública) y al desarrollo de una mayor orientación hacia el cliente. La innovación ha producido oferta tecnológica más variada y fácil de usar, que se ha visto acompañada de un esfuerzo por garantizar la seguridad de las transacciones realizadas a través de los canales a distancia.

Con un entorno favorable como el descrito, y dada la existencia de un sistema financiero profundo y altamente sofisticado, la explicación a la relativamente baja utilización de la banca *online* en España podría achacarse a un retraso en la ‘cultura digital’

frente a otros países europeos, pero no a una apuesta tímida por parte de las entidades de crédito. De hecho, aunque las inversiones realizadas han sido cuantiosas desde el lanzamiento del canal, el coste por transacción *online* es muy inferior al observado en el resto de los canales de distribución bancaria. Por lo tanto, el objetivo de las entidades de crédito pasa por incrementar el porcentaje de clientes que adopten el canal electrónico para realizar al menos una parte de sus transacciones. Las mejoras constantes en los servicios ofrecidos, así como la caída del precio de las conexiones de banda ancha y la aparición de nuevas posibilidades de acceso (telefonía móvil 3G) sugieren que el tiempo está jugando a favor de la banca *online* en España.

REFERENCIAS BIBLIOGRÁFICAS

- AFINET GLOBAL (2002-2007): «Servicio de benchmarking de banca online en España». Periodicidad anual.
- ANTI PHISHING WORKING GROUP (2008): «Phishing Activity Trends Report for the Month of December» (www.antifishing.org/reports/apwgeport_dec_2007.pdf)
- ASOCIACIÓN ESPAÑOLA DE BANCA (2007): «Anuario Estadístico 2006».
- BANCO DE ESPAÑA (2007): «Memoria del Servicio de Reclamaciones 2006».
- CALVO, A. y MARTÍN DE VIDALES, I. (2007): «El Escenario de la Banca por Internet en España (2000-2006)», Boletín Económico Información Comercial Española, 2919: 71-84, Madrid.
- CLIMENT, F. y MOMPALER, A. (2007): «La situación de la banca online en España». Boletín Económico de Información Comercial Española, 2898: 27-49, Madrid.
- COMISIÓN DEL MERCADO DE LAS TELECOMUNICACIONES (2007): «Nota Mensual – Noviembre 2007»
- CONFEDERACIÓN ESPAÑOLA DE CAJAS DE AHORROS (2007): «Informe Anual 2006».
- CONSEJO ASESOR DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (2005): «Ponencia del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información. Informe final».
- (<http://www.planavanza.es/NR/rdonlyres/04E8C3BF-DE54-4209-9829-E244F19B711F/14442/INFORMEFINALPONENCIACATSI.pdf>)
- EUROSTAT (2007): «Information Society Statistics: Computers and Internet in households and enterprises».
- FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (2005): «Authentication in an Internet Banking Environment» (http://www.ffiec.gov/pdf/authentication_guidance.pdf)
- FUNDACIÓN ORANGE (2007): «Informe España 2007». Colección Fundación Orange. Director: Manuel Gimeno.
- HENG, S., MEYER, T. y STOBBE, A. (2007): «Be a driver, not a passenger. Implications of Web 2.0 for financial institutions». Deutsche Bank Research.
- INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (2008): «Segunda Oleada del Estudio sobre la seguridad de la información y eConfianza de los hogares españoles».
- RSA SECURITY (2008): «RSA Online Fraud Report». (http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0208.pdf)
- SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN: «Plan Avanza». (<http://www.planavanza.es>)