



CONCLUSIONES RELATIVAS AL PLAN DE INSPECCIÓN DE OFICIO AL SECTOR DE LA BANCA A DISTANCIA CON OBJETO DE VERIFICAR EL GRADO DE ADECUACIÓN DE SUS FICHEROS DE *CLIENTES Y CLIENTES POTENCIALES* A LA LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1. INTRODUCCIÓN

Por acuerdo del Director de la Agencia de Protección de Datos (APD), se procedió durante el año 2001 a realizar un Plan de Inspección de oficio al sector de la Banca a Distancia con objeto de comprobar el grado de adecuación de los ficheros automatizados del sector a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, Ley 15/1999, de 13 de diciembre (LOPD) y normativa que la desarrolla.

El objetivo principal perseguido en la realización del plan ha sido no tanto el auditar los tratamientos de datos personales en la actividad bancaria tradicional como el auditar aquellos tratamientos que son específicos y que derivan precisamente de una relación entre entidades y ciudadanos en la que no es necesaria una presencia física.

Es esta especial relación la que impone una serie de procedimientos que no existían en la banca tradicional y en los que las nuevas tecnologías juegan un papel fundamental, al tiempo que presentan una serie de implicaciones en materia de protección de datos y, especialmente, en los aspectos de seguridad, donde conseguir un equilibrio entre la necesidad de establecer procedimientos sencillos para el acceso del usuario a los servicios y la imprescindible seguridad en las transacciones, no resulta trivial.

No obstante lo anterior, también se recogen en el presente documento conclusiones y recomendaciones sobre algunos tratamientos de los que se ha tenido conocimiento en el transcurso de las auditorías y que no siendo específicos de la banca a distancia, se ha considerado que necesitan una adecuación a lo establecido en la normativa de protección de datos.

Para la consecución de este objetivo se ha seleccionado una muestra de entidades con la idea de exponer las conclusiones obtenidas de forma anónima, ya que lo que interesa es que las recomendaciones sirvan al sector en su conjunto para adecuar su funcionamiento a la normativa de protección de datos.

Finalmente debe puntualizarse que el presente informe recoge fundamentalmente aquellos aspectos que son susceptibles de mejoras. Bien entendido que se trata de aspectos concretos obtenidos de entre todas las entidades analizadas, sin que pueda deducirse por ello que ninguna en particular presenta un funcionamiento deficiente así como tampoco el sector en su conjunto.



2 CONCLUSIONES RESPECTO DE LA LEY ORGÁNICA 15/1999 Y NORMATIVA DE DESARROLLO.

Las conclusiones relativas a los ficheros de clientes son las siguientes:

2.1 Origen de la información.

Atendiendo al origen de la información se han detectado tres fuentes básicas de datos personales:

- a) Datos personales procedentes de fuentes externas mediante alquiler y/o compra de ficheros con fines de publicidad directa.
- b) Datos facilitados a la entidad directamente por los afectados con el fin de solicitar algún tipo de información o participar en alguna iniciativa de aquella (simulador de bolsa, agregador financiero, etc.), pero que no llegan a disponer de un Código de Cuenta de Cliente (CCC) con la entidad.
- c) Datos de personas que tienen al menos un Código de Cuenta de Cliente (CCC) con la entidad.

Los datos personales obtenidos en base a la casuística anterior pueden ser ampliados con información procedente de otras fuentes:

- a) Información facilitada por el propio cliente cuando solicita la contratación de productos y servicios ofrecidos por la entidad (ej.: solicitud de un crédito hipotecario, etc.)
- b) Información recabada por los propios agentes comerciales de la entidad bancaria.
- c) Información financiera de productos contratados, así como movimientos en las cuentas.
- d) Información procedente de otras entidades financieras (por ejemplo, la obtenida como consecuencia de los agregadores financieros).
- e) Información sobre incumplimiento de obligaciones dinerarias obtenida de ficheros constituidos al amparo del artículo 29 de la LOPD.
- f) Información relativa al comportamiento de pago en los productos de activo contratados con la propia entidad.



2.2 Calidad de datos (artículo 4).

- Respeto de la finalidad de los tratamientos:

De la información recabada de los ficheros de gestión de clientes se desprende que los datos personales tratados en cada uno de ellos son, en general, adecuados, pertinentes y no excesivos con las correspondientes finalidades.

Se ha detectado también la existencia de sistemas de información del tipo *DataWarehouse* o CRM especializados en tratamientos complejos y masivos de la información de los usuarios. No obstante, no se ha detectado la utilización de estos sistemas para la realización de perfiles personales individualizados, sino para la obtención de datos agregados sobre el comportamiento y aceptación de los productos y servicios ofrecidos por la entidad, así como para la selección del conjunto de clientes a los que ofrecer un determinado producto o servicio.

- Respeto de la exactitud de los datos:

En general, los datos de los usuarios son exactos y se encuentran actualizados.

No obstante, se ha detectado el caso de alguna entidad que almacena en el sistema de análisis de riesgos asociado a las solicitudes de créditos, el resultado de las consultas a ficheros de incumplimiento de obligaciones dinerarias constituidos al amparo del artículo 29 de la LOPD. En el caso encontrado, la entidad no procede a actualizar dicha información ni a borrarla una vez se finaliza la tramitación de dicha solicitud, por lo que se corre el riesgo de que con el paso del tiempo la información recabada no responda con veracidad a la situación actual del afectado, por lo que podría incurrir en un incumplimiento del artículo 4.3 de la LOPD.

- Respeto de la cancelaciones de datos:

El procedimiento establecido en la práctica en las entidades analizadas consiste en que cuando un cliente procede a la cancelación de todas sus cuentas sin que haya solicitado explícitamente la cancelación de sus datos personales, la entidad procede a cancelar dichas cuentas pero conservando todos sus datos personales con el fin de acreditar la existencia de la relación contractual durante los plazos legales previstos. En algunos casos la entidad procede de forma adicional a excluirle de futuras promociones comerciales, no así en otros casos, al considerar la entidad que puede seguir prestándole su actividad.

En el caso de que el cliente haya solicitado además la cancelación de sus datos personales, la entidades proceden a bloquear dichos datos mediante su marcado, restringiendo, en todo caso, su futura inclusión en campañas comerciales.



Durante el proceso de alta como cliente no siempre llega a producirse un alta efectiva del mismo, quedando el proceso interrumpido cuando no paralizado indefinidamente sin que quede activada la cuenta del cliente. En este sentido, se ha detectado que algunas entidades no cancelan en ningún momento los datos de aquellos solicitantes para los cuales no se completó el proceso.

2.3 Derecho de información en la recogida de datos y consentimiento del afectado (artículos 5 y 6).

En general, la persona que se dirige a una entidad del sector recibe información acerca del tratamiento de sus datos por distintas vías: Internet, teléfono y a través del contrato en papel de apertura de cuenta.

La información facilitada a través de Internet y de los contratos recoge que los datos recabados van a ser incorporados a un fichero, indicando la denominación social y dirección del responsable del mismo, así como de la posibilidad que tiene la persona de ejercer sus derechos de acceso, rectificación y cancelación en consonancia con la LOPD.

Se ha detectado, en alguna ocasión, que la información facilitada difiere dependiendo del medio consultado o que se encuentra diseminada en diferentes ubicaciones sin que ninguna de ellas recoja la totalidad. En un caso concreto figura incluso información que puede ser contradictoria: a través de Internet se informa de posibles cesiones a un grupo de empresas y a través de los contratos en papel de posibles cesiones a otro grupo de empresas diferente.

Así mismo, y en relación con lo anterior, también se ha detectado que la información no siempre resulta fácilmente accesible para el usuario por no estar integrada en el proceso de recogida de los datos personales.

En general, y en relación con el artículo 30 de la LOPD, la información que se ofrece a clientes y potenciales clientes recoge que se van a utilizar sus datos con fines comerciales para ofrecer productos financieros. No obstante, dicha información no va, por lo general, acompañada de un mecanismo que permita oponerse a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

En relación también con el artículo 11 de la LOPD, se ha detectado la práctica de incluir cláusulas que informan de forma genérica sobre cesiones a “*empresas del grupo*” para “*la oferta y contratación de otros productos y servicios*” sin que se concrete con mayor detalle la información aportada y sin que se recoja en el propio contrato ningún procedimiento que permita expresar dicha oposición, como por ejemplo la inclusión de una casilla al efecto.

Otro aspecto a señalar es que no siempre se especifican cuales de los datos recabados son obligatorios y cuales no. Así, por ejemplo, una entidad recoge el



dato del número de hijos sin especificar si es voluntario o no y cual es la finalidad de recabar dicha información.

También, se ha detectado la realización de segmentaciones o perfiles de clientes con fines comerciales, a partir de la información personal y comercial que consta en los ficheros de la entidad, sin que se informe de ello a los clientes y sin que éstos puedan, por lo tanto, oponerse a dicho tratamiento.

Las entidades analizadas utilizan como práctica habitual grabar las conversaciones que se producen en los accesos a través de los servicios telefónicos. Es práctica general que se informe de ello a los clientes a través de las condiciones contractuales.

Finalmente, cabe señalar la prestación, por parte de algunas entidades, del servicio denominado *Agregador Financiero* por el cual la entidad ofrece al usuario la posibilidad de acceder a través de una única consulta a todas las posiciones que el usuario pueda tener con diferentes entidades financieras. Para ello, el usuario debe de facilitar a la entidad prestataria del servicio las claves de acceso a las restantes entidades financieras.

2.4 Datos especialmente protegidos (artículos 7 y 8).

No se ha constatado la existencia de datos especialmente protegidos en los ficheros de clientes y potenciales clientes de las entidades analizadas.

2.5 Seguridad de los datos (artículo 9 y RD 994/1999)

Uno de los aspectos esenciales y más significativos de la banca a distancia es precisamente la identificación y autenticación de los clientes dado que no existe presencia física de los mismos. Por esta razón, se habilitan procedimientos técnicos para que de forma remota los clientes puedan consultar sus posiciones e incluso realizar transacciones económicas y contratar productos financieros.

En este sentido, se han analizado dos situaciones consideradas especialmente relevantes: el proceso de contratación a distancia de la cuenta de cliente y el acceso a distancia del cliente a los productos y servicios que le ofrece la entidad.

Respecto del proceso de alta como cliente, se inicia básicamente mediante una petición realizada por el solicitante ya sea por teléfono o por Internet, donde tras aportar ciertos datos básicos iniciales la entidad asigna ya un Código de Cuenta de Cliente en estado de preactivado, así como las claves de identificación y autenticación en los casos en los que el usuario puede elegirlos, desencadenándose a continuación un proceso de remisión de documentación y de las claves al titular o titulares.

Para la remisión de las claves se utilizan, en general, servicios de mensajería con acuse de recibo e identificación fehaciente de destinatario, o, en su defecto,



correo ordinario con mecanismos posteriores de activación, por lo que resultan adecuados dichos procedimientos al identificar inequívocamente al cliente.

Seguidamente, se inicia un proceso de recogida y seguimiento de la documentación que debe remitir el cliente a la entidad (contrato firmado, fotocopia del NIF, etc.). Si este proceso no llega a completarse no se activa la cuenta del cliente.

Respecto del acceso a distancia del cliente a los productos y servicios que le ofrece la entidad, se constata la existencia de tres estadios distintos: la identificación, la autenticación y la firma.

La identificación permite a la entidad saber quien es el cliente que se pone en contacto con ella y se produce mediante la aportación (telefónica o por Internet) de un código de usuario o secuencia alfanumérica de entre 6 y 15 caracteres que es única para cada cliente (en ocasiones se utiliza como código de usuario el NIF de la persona e incluso, en algún caso y por teléfono, basta con aportar el número de teléfono del cliente y su nombre). Siempre que se facilita el código de identificación a través del teléfono queda registrado en las grabaciones de las conversaciones de los operadores.

La autenticación es el primer control que realiza la entidad para garantizar que la persona que se ha identificado es quien dice ser. La autenticación se produce mediante la aportación de una parte o de la totalidad de una clave de autenticación formada por entre 4 y 12 caracteres alfanuméricos y que, en principio, únicamente debiera conocer el cliente y el sistema de gestión de claves de la entidad. Cuando se elige a través de teléfono queda registrada en las grabaciones de las conversaciones con los operadores.

Una vez superada la identificación y autenticación, es práctica general que la entidad permita al cliente consultar sus posiciones, así como solicitar la realización de operaciones que suponen movimientos de capital: transferencias, contratación de otros productos, etc. Para poder culminar estas operaciones, en las que se produce un cambio en las posiciones del cliente, la entidad exige además un control adicional o firma.

La firma se produce mediante la aportación de una parte si no la totalidad de una clave de firma que únicamente debe de conocer el cliente y el sistema de gestión de claves de la entidad. La clave de firma suele formarse por una secuencia alfanumérica de entre 8 y 12 caracteres o bien mediante una tarjeta que contiene impresos una serie de secuencias numéricas. A través del teléfono se puede solicitar su emisión e incluso su cambio pero no asignarla de viva voz a través de un operador que conozca la identificación del cliente.

En teoría, la arquitectura de claves establecida por las entidades ofrece seguridad. No obstante, en la práctica pueden aparecer ciertas situaciones que puedan presentar algún riesgo, no tanto por la tecnología utilizada, como por los procedimientos establecidos sobre dicha tecnología, así como, por la



información facilitada a los usuarios en algún caso, o por la conducta de los propios usuarios en otros.

Se trata, en consecuencia, de establecer un equilibrio entre la consistencia del sistema de autenticación utilizado por un lado y la capacidad de asimilación del cliente por otro. En este sentido sería conveniente que las entidades facilitasen al cliente información sobre los sistemas de cifrado: sus riesgos y las formas de disminuirlos, como por ejemplo, la buena práctica de seleccionar claves que contengan letras y números, que la clave no contenga información que identifique a la persona (número de teléfono, nif, fecha de nacimiento, etc.), así como la conveniencia de cambiar las claves cada cierto tiempo. En este sentido, es muy importante la información que las entidades facilitan al cliente al respecto, comprobándose que dicha información puede ser mejorada.

Por otro lado, se han constatado también determinadas situaciones puntuales que son susceptibles de mejoras en algunas entidades y que se relacionan a continuación. Bien entendido, como se ha señalado anteriormente, que dichas situaciones no se producen acumulativamente en las entidades analizadas, sino puntualmente en unas u otras.

- Respecto de la información facilitada por la entidad, se ha encontrado una situación en la que operadores de una entidad conminaban a los clientes, durante el proceso de alta, a que seleccionasen como clave su propia fecha de nacimiento. Esta práctica introduce riesgos sobre todo cuando dicha clave no se utiliza en su conjunto sino a través de posiciones de la misma ya que, en este caso, determinadas posiciones son fácilmente predecibles.
- También, respecto de la información facilitada por las entidades, se ha constatado como en el contrato de una de ellas se afirma que las claves únicamente son conocidas por el usuario, cuando la realidad es que las claves de identificación y de autenticación, para dicha entidad, han de ser facilitadas en su totalidad, además, al operador de acceso telefónico.
- Otra situación detectada consiste en utilizar exactamente los mismos procedimientos sobre las mismas claves, incluida la de firma, para el acceso a través del operador telefónico y a través de Internet, lo que puede llevar a que dicho procedimiento no identifique de forma inequívoca y personalizada al usuario. En este sentido hay que tener en cuenta que las operaciones realizadas por los empleados de las entidades quedan registradas cuando son realizadas desde los ordenadores de la entidad, por lo que pueden depurarse fácilmente responsabilidades, no siendo así en el caso de un empleado desleal que, conociendo las claves de un cliente, le suplante desde los canales telefónicos e Internet establecidos para la comunicación entre cliente y entidad.
- En relación con el punto anterior, algunas entidades solicitan en los accesos por Internet, y cuando no es por tarjeta de claves, posiciones de la clave de autenticación y de la de firma. Esta práctica tiene sentido en los accesos a través del teléfono, ya que impide que el operador conozca las claves



completas del cliente. Sin embargo, en los accesos por Internet, cuando se solicitan posiciones aleatorias de las claves y no la clave completa se introduce un factor adicional de riesgo sin que se facilite por ello la labor al cliente.

- Algunas entidades solicitan de forma reiterada los valores erróneos o no contestados por el supuesto cliente relativos a las posiciones concretas de su clave o tarjeta de claves, reiterándose dicha solicitud hasta que se facilite correctamente o se bloquee la cuenta como consecuencia de los errores acumulados. Sin embargo, no todas las entidades siguen dicha práctica, y en su lugar, y ante la situación planteada, solicitan una nueva posición aleatoria, lo que puede ser utilizado en su beneficio por quien pretenda suplantar a un cliente al conocer algunas de las posiciones de su clave o tarjeta de claves.
- Por lo general, el cliente puede cambiar las claves de autenticación y la de firma y en la mayoría de los casos incluso elegir las. En este caso, si la elección se realiza por vía telefónica el operador conoce la clave (en los casos detectados, al menos la clave de autenticación) pese a que en el contrato entre entidad y cliente se afirma que las claves sólo son conocidas por el cliente. En estos casos sería conveniente habilitar un procedimiento que impida que el empleado conozca la totalidad de la clave.
- Otra situación detectada se produce durante el cambio de la clave cuando se realiza a través del teléfono. En estos casos, el procedimiento habitual establecido para el cambio de la clave de firma consiste en dividir la tarea entre dos operadores de grupos distintos: uno del grupo de atención general y otro del grupo de seguridad. El primero de los operadores conoce la identificación de la persona, mientras que el operador de seguridad conoce la clave elegida por el cliente, existiendo como nexo entre ambos operadores un número que ambos operadores conocen (este mecanismo se denomina “*pantalla ciega*” ya que el operador de seguridad no tiene acceso a ningún dato personal del cliente). Este mecanismo presenta el riesgo de que el acuerdo de dos operadores permitiría realizar una transferencia sin que los rastros de auditoría señalaran nada anómalo.

En relación con lo anterior, se considera que las siguientes políticas contribuyen a disminuir los riesgos existentes en las situaciones detectadas:

- Que las entidades faciliten a los clientes información acerca de la buena práctica de gestión de claves: como la conveniencia de seleccionar claves que contengan letras y números y que preferiblemente no tengan una relación directa con la persona (número de teléfono, nif, fecha de nacimiento, etc.), la idoneidad de cambiar las claves con cierta frecuencia, y en general todos aquellos aspectos que contribuyan a preservar la confidencialidad de las mismas.
- Que los operadores del canal telefónico no recaben claves completas del cliente si éste se encuentra identificado para ellos, así como, que se diferencien los accesos a través de los canales telefónico e Internet de forma



que no se utilicen los mismos procedimientos de acceso sobre las mismas claves. Todo ello, con el fin de evitar que a través de empleados desleales se pueda producir una suplantación del cliente sin que de ello quede constancia en los ficheros de la entidad.

- Que se soliciten de forma reiterada los valores erróneos o no contestados por el supuesto cliente relativos a las posiciones concretas de su clave o tarjeta de claves, reiterándose dicha solicitud hasta que se facilite correctamente o se bloquee la cuenta como consecuencia de los errores acumulados. Con ello se disminuye el riesgo de que un tercero, con conocimiento sobre una parte de la clave, pueda realizar un acceso no autorizado.

Finalmente, no se ha detectado en las entidades analizadas la utilización de esquemas de certificación y firma electrónica tipo PKI (Infraestructura de Clave Pública) para el acceso de los clientes a los servicios ofrecidos por las entidades analizadas. Estos esquemas de seguridad, aun no siendo legalmente exigibles, ofrecen la garantía de disponer de certificados realizados por terceros, garantizando determinados niveles de seguridad.

2.6 Deber de secreto (artículo 10).

En las relaciones contractuales que rigen las prestaciones de servicios para las entidades analizadas y que implican el acceso por parte de las empresas prestatarias a los datos personales de clientes de las entidades, se recogen cláusulas que exigen la debida confidencialidad sobre los datos a los que se accede.

No obstante, se han detectado entidades que no recogen en los contratos con su personal cláusulas que les obliguen a guardar el deber de secreto respecto de los datos personales a los que tengan acceso como consecuencia de su trabajo en la entidad.

También se ha detectado el caso de una entidad donde en la página *web* que se utiliza para el alta del cliente, se facilitan determinados datos personales a partir únicamente del correspondiente NIF de la persona, lo que permite conocer a cualquiera si una persona es o no cliente de dicha entidad, y en su caso, sus datos identificativos.

2.7 Cesiones de datos (artículo 11).

Si bien no se han detectado en las entidades inspeccionadas cesiones de datos a terceros, sí se ha constatado, como ya se ha indicado anteriormente en el apartado 2.3, algunos contratos con cláusulas que informan de forma genérica sobre cesiones a “*empresas del grupo*” para “*la oferta y contratación de otros productos y servicios*”, sin que se concrete más la información aportada haciendo referencia a las finalidades de la cesión y sin que se recoja en el propio



contrato ningún procedimiento que permita expresar la oposición a dicha cesión, como por ejemplo la inclusión de una casilla al efecto.

2.8 Acceso a los datos por cuenta de terceros (artículo 12).

En general, la mayoría de las prestaciones de servicios analizadas se encuentran plasmadas en contratos por escrito que recogen la finalidad de la prestación, siendo habitual que recojan dichos contratos lo estipulado en el artículo 12 de la LOPD.

No obstante, se han detectado algunos contratos que no recogen todos los requisitos exigidos en el artículo 12 de la LOPD como por ejemplo las medidas de seguridad a que se refiere dicho artículo y que el encargado del tratamiento está obligado a implementar, o el destino final de los datos personales una vez ha finalizado la prestación contractual, entre otros.

2.9 Impugnación de valoraciones (artículo 13).

No se han detectado en las entidades estudiadas que se tomen decisiones con efectos jurídicos que afecten a personas físicas y que tengan como fundamento únicamente un tratamiento de datos destinado a evaluar determinados aspectos de la personalidad del individuo.

No obstante, conviene señalar que algunos de los tratamientos analizados, como por ejemplo los de *scoring*, si que podrían, en determinadas circunstancias, llevar a tomar decisiones automáticas teniendo como fundamento únicamente un tratamiento sobre aspectos de la personalidad. En este sentido, dichos tratamientos quedarían plenamente sujetos a lo prevenido en el citado artículo.

2.10 Derecho de las personas: acceso, rectificación, cancelación y oposición. (artículos 15 y 16).

Las entidades inspeccionadas informan a los usuarios de la posibilidad de ejercer estos derechos al tiempo que cuentan con procedimientos definidos para su ejercicio, siendo habitual que dichos procedimientos recojan lo dispuesto en la Instrucción 1/1998 de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Se ha constatado que el derecho ejercido mayoritariamente por los usuarios de estos servicios de manera formal es el derecho de oposición al tratamiento de sus datos personales con fines de promoción comercial.



2.11 Creación, notificación e inscripción en el Registro de la APD (artículos 25 y 26).

Las entidades analizadas han procedido a la inscripción en el Registro General Protección de Datos de la APD de sus ficheros de clientes y potenciales clientes.

2.12 Datos incluidos en fuentes accesibles al público (artículo 28).

Si bien las entidades analizadas no publican ningún repertorio susceptible de considerarse fuente accesible al público, sí se ha constatado la realización, por parte de aquellas, de compras o alquileres de datos personales suministrados por terceros y cuyo origen último resultan fuentes accesibles al público, siendo utilizados dichos datos con fines de publicidad y de prospección comercial.

En este sentido se han detectado dos modalidades de actuación bien diferenciadas:

- a) En unos casos, la entidad financiera procede al alquiler de listados para usos concretos a empresas especializadas en suministrar direcciones procedentes de fuentes accesibles al público. La solicitud de datos se realiza en base a diferentes criterios socioeconómicos y demográficos facilitados por las empresas suministradoras y que obtienen del cruce de los datos personales básicos que figuran en diferentes fuentes de acceso público con datos socioeconómicos agregados en función de datos geográficos.

En estos casos, la entidad recibe un listado que contiene básicamente nombre, apellidos, sexo y domicilio, a partir del cual se confecciona un mailing promocional, procediendo posteriormente al borrado de dicho listado, no quedando datos personales del listado en los ficheros de la entidad.

- b) En otros casos, la entidad financiera procede a la constitución de un fichero propio con un gran volumen de registros mediante la acumulación de diferentes compras de ficheros a lo largo del tiempo. La finalidad de este fichero no es la de realizar una campaña concreta sino la de servir de base para la realización de diferentes campañas, como por ejemplo envíos promocionales nominativos a los domicilios del área de influencia de una sucursal bancaria, etc.

Dentro de esta última modalidad se ha detectado una entidad cuyo fichero presenta una doble problemática:

En primer lugar, y relacionado con la antigüedad de los datos, cabe señalar que la LOPD introduce respecto de las fuentes accesibles al público un carácter temporal. En este sentido, el artículo 28.3 establece que *“Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico,*



ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.”.

Por lo expuesto, el citado fichero corre el riesgo de recoger actualmente datos que si bien originariamente quedaban amparados por proceder de fuentes accesibles al público, en la actualidad pueden haber perdido dicho amparo, ya sea por haber sido cancelados de las mismas o por haber perdido éstas dicho carácter.

En segundo lugar, y relacionado con la estructura de datos del fichero, cabe señalar que la estructura diseñada es mucho más amplia que la necesaria para albergar el fichero, lo que ha propiciado un enriquecimiento de los datos en algunos registros en los que, si bien en un porcentaje mínimo, se recogen datos que difícilmente tienen su origen en fuentes accesibles al público y sobre los que pudiera no existir el correspondiente consentimiento dado que no existe relación contractual con dichas personas. Entre estos datos se encuentran por ejemplo el DNI, tipo de vivienda, estado civil, número de hijos, tipo de actividad particular, profesión, país de nacimiento, país de residencia, nivel académico, indicador de fallecido, etc.

2.13 Prestación de servicios de información sobre solvencia patrimonial y crédito (artículo 29).

En general, la mayoría de las entidades disponen de acceso a ficheros comunes relativos al incumplimiento de obligaciones dinerarias, comunicando al fichero común los impagos producidos y consultando en el fichero común las posibles deudas de sus clientes. En general, las entidades consultan estos ficheros como parte de un tratamiento de análisis de la solvencia del cliente cuando se produce la contratación de algún producto financiero con riesgo económico para la entidad (contratación de productos de activo, emisión de tarjetas, etc.).

Así por ejemplo, se ha detectado el caso de una entidad donde la apertura de la primera cuenta va asociada a la emisión de una tarjeta de débito al primer titular, por lo que la entidad procede de forma sistemática a realizar un análisis de solvencia de todos los primeros titulares. Dicho análisis es repetido en ocasiones con el fin de excluir a clientes de determinadas campañas comerciales en las que se promocionan determinados productos de activo.

2.14 Tratamientos con fines de publicidad y de prospección comercial (artículo 30).

En las entidades analizadas se ha detectado que existe un procedimiento establecido para excluir de la remisión de publicidad a aquellos clientes que han ejercido su derecho de oposición. Se constata además, que la oposición a este tratamiento es el principal derecho ejercido por los usuarios de los servicios bancarios.



Como ya se ha señalado en el apartado 2.3, en general se informa que los datos recabados se van a utilizar con fines comerciales para promociones de productos financieros. No obstante, dicha información no va por lo general acompañada de un mecanismo que permita oponerse a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

2.15 Movimiento internacional de datos: Norma general y Excepciones (artículos 33 y 34).

No se ha detectado que se realicen transferencias internacionales de datos en las entidades bancarias inspeccionadas que no estén amparadas por la excepción d) del artículo 34.

3 RECOMENDACIONES A LAS ENTIDADES DE BANCA A DISTANCIA.

A tenor de lo expuesto, y en atención al resultado de las actuaciones practicadas por parte de la Inspección de Datos, se han observado ciertas deficiencias en los Sistemas de Información de entidades que se dedican a la denominada banca a distancia en relación al cumplimiento de las prescripciones de la Ley Orgánica 15/1999 y su normativa de desarrollo, cuya subsanación supondría una sustancial mejora en el acatamiento del citado marco normativo.

Por lo tanto, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga en artículo 5 c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, dicta las siguientes **RECOMENDACIONES** que deberán ser observadas por las entidades de este sector, al objeto de adecuar los tratamientos automatizados que realizan a los principios de la normativa vigente en materia de protección de datos de carácter personal.

PRIMERA: En relación con la calidad de los datos personales (artículo 4 de la LOPD).

Respecto de la incorporación a los propios sistemas de la entidad de datos procedentes de ficheros de incumplimiento de obligaciones dinerarias constituidos al amparo del artículo 29 de la LOPD, debe distinguirse según que la información se refiera o no a clientes. Respecto de los clientes de la entidad financiera los datos obtenidos de ficheros regulados en el artículo 29 de la LOPD no resulta necesario que sean actualizados si se mantienen en ficheros que, no siendo de morosidad, incluyan otras informaciones personales del cliente. Por el



contrario, en el caso de personas que no son clientes de la entidad o, en el de clientes de la entidad cuyos datos se incorporan a ficheros de solvencia patrimonial y crédito, se recomienda que, o bien se proceda a la cancelación de la citada información una vez se haya tramitado la solicitud de crédito, o en su defecto se habiliten los controles y procedimientos pertinentes para que dicha información sea exacta y puesta al día de forma que responda con veracidad a la situación actual del afectado tal y como establece el artículo 4.3 de la LOPD

En relación a la cancelación de los datos personales cabe señalar que si bien existen obligaciones legales de mantener ciertos conjuntos de datos durante determinados períodos de tiempo (cinco años para finalidad fiscal, etc.), no debe extrapolarse dicha obligación a la totalidad de los datos que se tengan de una persona, como por ejemplo los datos de marketing, por lo que aquellos datos cuyo mantenimiento no cuente con amparo legal, deberán ser suprimidos, no siendo suficiente en este caso el bloqueo de los mismos en consonancia con lo establecido en el artículo 16.3 de la LOPD.

Respecto del proceso de alta como cliente, debiera establecerse un plazo razonable desde la apertura de dicho proceso, transcurrido el cual, se cancele toda la información de aquellos solicitantes que no hubieren llegado a completar su alta.

SEGUNDA: En relación con el derecho de información en la recogida de datos y el consentimiento (artículos 5 y 6 de la LOPD).

El artículo 5 de la LOPD establece que *“los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”*.

La información facilitada durante la recogida de los datos es la base del consentimiento inequívoco requerido, como principio general, por el artículo 6 de la LOPD. Si bien las entidades analizadas proporcionan información, no siempre ésta recoge todos los aspectos contemplados en la normativa de protección de datos.

Por lo tanto, deberá establecerse un sistema que contraste la coherencia e integridad de la información facilitada a través de los diferentes medios utilizados por la entidad. De hecho, sería deseable que independientemente del medio consultado, la información fuese la misma. Dicha información deberá incluirse de forma obligatoria como parte integrante del proceso de recogida de datos personales, de forma que resulte fácilmente accesible para el usuario.



De no unificarse la información y en tanto en cuanto se faciliten informaciones distintas según el medio utilizado para recabar los datos, las entidades deberán adoptar las medidas necesarias para evitar en cada caso los tratamientos de datos o cesiones de los que no se hubiere informado a cada afectado.

Deberá especificarse qué información de la recabada se considera obligatoria y que información se considera voluntaria, siendo declarada como obligatoria la que resulte adecuada pertinente y no excesiva para la prestación del servicio contratado. En el caso de recabar información adicional voluntaria deberá especificarse la finalidad de la misma.

Deberá también informarse al cliente de los tratamientos que tengan como finalidad la realización de segmentaciones o perfiles de clientes con fines comerciales, así como establecer un procedimiento fácil y directo que permita ejercer la oposición a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

Respecto de los servicios de *agregadores financieros* sería conveniente que la entidad prestataria del servicio se limitara exclusivamente a presentar la información de las posiciones de los usuarios en las entidades previamente establecidas, procediendo a cancelar dicha información en cuanto deje de ser necesaria. Cualquier otro tratamiento que la entidad prestataria del servicio desee realizar deberá contar con el consentimiento previo e informado del usuario ofreciendo siempre la posibilidad de oponerse al mismo mediante un procedimiento fácil y directo como la inclusión de una casilla al efecto.

TERCERA: En relación con la Seguridad de los Datos Personales. (artículo 9 de la LOPD y RD 994/1999)

La Ley Orgánica 15/1999, en su artículo 9 dispone que *“El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.”*

El Real Decreto 994/1999, de 11 de junio de 1999, aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, que se clasifican en tres niveles atendiendo a la naturaleza de la información tratada y a la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.



De acuerdo a lo establecido en el citado Reglamento, las entidades deberán cumplir las medidas de seguridad aplicables a cada uno de los ficheros en función de su clasificación como ficheros de nivel básico y medio.

Respecto de las medidas de seguridad y especialmente en relación con el artículo 18 del citado Reglamento, se recomienda que se diseñen los mecanismos de identificación establecidos de forma que garanticen que la identificación del usuario que intenta acceder al sistema es inequívoca y personalizada, dado que se han detectado situaciones que aunque por si solas y de forma aislada no representan fallos de seguridad sí que pueden contribuir, ya sea por acumulación de varias o por combinación con otros factores, a que los mecanismos de identificación no garanticen dicha identificación en los términos establecidos en el citado artículo.

CUARTA: En relación con el deber de secreto (artículo 10 de la LOPD).

Se recomienda incluir en los contratos de trabajo cláusulas relativas al deber de secreto respecto de los datos personales a los que tienen acceso los empleados como consecuencia de su actividad, ya sean los propios empleados de la entidad como los empleados de las empresas prestatarias de servicios para la entidad con acceso a los datos personales de los clientes.

Se recomienda también que las páginas web de acceso a los servicios se diseñen de tal manera que no proporcionen al usuario más datos personales que los introducidos por el propio usuario, hasta que éste no haya superado con éxito los controles de identificación y autenticación.

QUINTA: En relación con la cesiones de datos (artículo 11 de la LOPD).

La Ley Orgánica 15/1999, en su artículo 11.1 establece que *“Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”*.

Respecto del consentimiento, el artículo 11.3 de la misma Ley puntualiza que *“Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar”*.

Si bien las entidades analizadas han manifestado no realizar cesiones de datos a terceros, lo cierto es que en la información que algunas de ellas facilitan a los clientes figuran cláusulas tipo que informan de la posibilidad de efectuar cesiones a *“empresas del grupo”* para *“la oferta y contratación de otros productos y servicios”*, sin especificar ni las empresas ni los sectores de actividad a que pertenezcan las mismas y sin que éstos sectores puedan



deducirse en base a la naturaleza de los productos y servicios que pudieran ofertarse.

En relación con cláusulas como la apuntada cabe señalar que su contenido resultaría insuficiente, ya que no permite conocer la finalidad a que se destinarían los datos cedidos o el tipo de actividad de aquel a quien se pretenden comunicar, por lo que dicho consentimiento sería nulo a tenor de lo recogido en el artículo 11.3 de la LOPD. En definitiva, y como establece el artículo 4.1 de la LOPD, las finalidades para las que se recaben datos han de ser determinadas, explícitas y legítimas.

Por lo expuesto, en caso de que se prevea la realización de cesiones a otras empresas deberá recabarse con carácter previo a la cesión el correspondiente consentimiento en los términos establecidos en la Ley. Igualmente, la cláusula por la que se informa de la posibilidad de la cesión de los datos personales a terceros deberá recoger un procedimiento que permita al interesado expresar su oposición, como por ejemplo la inclusión de una casilla al efecto.

SEXTA: En relación con el acceso a los datos por cuenta de terceros (artículo 12 de la LOPD).

Se ha detectado en todas las entidades auditadas la existencia de contratos con terceros para la prestación de servicios que conllevan el acceso a determinados ficheros por parte de las terceras empresas, prestadoras de servicios.

En este sentido, el artículo 12 de la LOPD en sus apartados segundo y tercero, establece que: *“2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.”*

Como ya se ha mencionado en las conclusiones, en general, la mayoría de las prestaciones de servicios analizadas se encuentran plasmadas en contratos por escrito que recogen la finalidad de la prestación, siendo habitual que recojan dichos contratos lo estipulado en el artículo 12 de la LOPD, si bien se han detectado algunos contratos en los que no se recogen todos los requisitos exigidos en el citado artículo.



Por todo ello, con objeto de conseguir una mejor adecuación de los tratamientos automatizados a los principios de la normativa de protección de datos, los contratos de prestación de servicios establecidos con terceros deben adecuarse a lo previsto en el artículo 12 de la LOPD.

A estos efectos, se recomienda que en las prestaciones de servicios que tengan por objeto la realización de un tratamiento de datos por parte de un tercero, la entidad debe tener en cuenta, como responsable del fichero, lo siguiente:

- a) La prestación habrá de plasmarse en un contrato, que deberá constar por escrito, y que establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a la normativa española de protección de datos.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento

- b) La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

Por otra parte, aunque en la inspección practicada no se ha detectado que se lleven a cabo subcontrataciones, la experiencia ha demostrado la frecuencia con que las empresas prestadoras de servicios a terceros suelen subcontratar con otras empresas parte del servicio a prestar.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la prestadora del servicio subcontrate a su vez esta segunda actividad con otra empresa, a menos que la prestadora actúe en nombre y por cuenta del responsable del fichero.

SÉPTIMA: En relación con los datos procedentes de fuentes accesibles al público con fines de publicidad y prospección comercial (artículo 28 de la LOPD).

En este sentido, en el caso de datos procedentes de fuentes accesibles al público, deberán establecerse los controles pertinentes para garantizar la actualización de los datos, de forma que se tenga en cuenta el carácter temporal de la fuente de acceso público, en consonancia con lo estipulado en el artículo 28.3 de la LOPD.

Adicionalmente, las entidades que habiendo constituido un fichero a partir de datos obtenidos de fuentes accesibles al público con fines de publicidad y prospección comercial y que procedan a incorporar datos adicionales, no



AGENCIA DE PROTECCIÓN DE DATOS
SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS

procedentes de fuentes accesibles al público, habrán de tener en cuenta los requerimientos establecidos en la normativa de protección de datos para el tratamiento de dichos datos y, en particular, la necesidad de contar con el consentimiento informado del afectado.

OCTAVA: En relación con los tratamientos con fines de publicidad y de prospección comercial (artículo 30 de la LOPD).

En los casos en que se vayan a tratar datos personales para la promoción comercial de productos y servicios de entidades distintas de aquella con la que se ha establecido una relación contractual, en el momento en que se recaben datos personales deberá informarse de las finalidades específicas para las que van a ser utilizados tales datos, debiendo habilitarse un mecanismo que permita al usuario, en ese momento, poder dejar constancia de su oposición a dicho tratamiento, como por ejemplo la inclusión de una casilla al efecto.

Madrid, 12 de julio de 2002

EL DIRECTOR DE LA AGENCIA
DE PROTECCIÓN DE DATOS

Fdo. Juan Manuel Fernández López