

En forma de anexo, se presentan en esta Memoria las cifras y estadísticas correspondientes a la actividad de la Subdirección General de Inspección de Datos a lo largo del año 2006. A continuación, se analizan estos resultados numéricos y se presentan las principales conclusiones que cabe extraer de los mismos.

REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN

La documentación de salida que ha generado la Inspección a lo largo del año ha crecido sensiblemente con respecto al ejercicio anterior: en torno al 14%. Este incremento es fiel reflejo del crecimiento experimentado por las actuaciones y procedimientos tramitados en la Subdirección.

La documentación de entrada, por otra parte, creció un 10% en 2006 respecto a 2005, lo que supone una continuación en la tendencia creciente, si bien implica una desaceleración relativa respecto de las cifras de 2004 y 2005, que reflejaron crecimientos cercanos al 30%. Se consolidan los citados crecimientos, así como la tendencia ascendente en el uso de los servicios de la Agencia, cada vez más conocidos por la ciudadanía como consecuencia de la creciente divulgación de los principios de protección de datos de carácter personal.

ACTUACIONES Y PROCEDIMIENTOS INICIADOS (ÁREA DE INSPECCIÓN)

En relación con el año anterior, en 2006 se ha producido un crecimiento en las actuaciones previas de investigación realizadas como consecuencia de denuncia. Con respecto al año 2006, las actuaciones han experimentado un incremento cercano al 11%, consolidando así la tendencia de crecimiento que en 2004 llegó a ser del 70%. La actividad inspectora de la Agencia, por tanto, sigue creciendo. Debe tenerse en cuenta, además, la realización en 2005 de un plan sectorial de oficio a la enseñanza reglada no universitaria, que ha supuesto, no únicamente una importante utilización de recursos humanos y materiales, sino un importante revulsivo en la aplicación de los principios de protección de datos en el citado sector.

En 2006 continúa produciéndose una polarización numérica de actuaciones previas de investigación por sector de actividad. La suma del sector de entidades financieras y telecomunicaciones asciende al 56%. El tercer sector en importancia numérica, de acuerdo con lo expuesto con anterioridad, lo constituyen las Administraciones Públicas.

Dentro del sector financiero la mayoría de las actuaciones de investigación previa finalizadas se refieren al cumplimiento o incumplimiento de obligaciones dinerarias y, en particular, a la inclusión en ficheros de morosidad (63%). En la misma línea, en el sector de las telecomunicaciones, los asuntos relativos a un eventual incumplimiento de las obligaciones dinerarias constituyen el porcentaje mayor, con un 58%.

En lo que se refiere a Comunidad Autónoma del denunciante, se produce un incremento en las actuaciones previas iniciadas fuera de la Comunidad de Madrid. No obstante, esta Comunidad se mantiene en primera posición, con un 27%, seguida de Cataluña, que asciende de un 10% en 2005 a un 13% en 2006, y Andalucía, con un 11%.

En idéntica tendencia, las cifras correspondientes a las actuaciones previas de investigación clasificadas por la Comunidad Autónoma en la que tiene su sede el principal investigado establecen una predominancia especial a la Comunidad de Madrid, con un 60%, ocupando el segundo lugar Cataluña, con un 11%.

ACTUACIONES Y PROCEDIMIENTOS FINALIZADOS (ÁREA DE INSTRUCCIÓN)

En 2006 el número de actuaciones de inspección archivadas al no haberse obtenido indicios de infracción también se ha visto incrementado. Parecida tendencia presentan los acuerdos por los que se resuelven los procedimientos contradictorios, tanto los que culminan en el reconocimiento de la infracción (y, en su caso, la imposición de la correspondiente sanción) como los que tienen un resultado de exoneración. Una derivación necesaria de ambas tendencias es el aumento correlativo de los recursos de reposición.

Los procedimientos que han experimentado un mayor crecimiento son los relativos a una posible infracción por parte de las Administraciones Públicas, que crecen más de un 400% respecto a 2005.

Únicamente se produce un descenso en el número de Resoluciones de los procedimientos de tutela de derechos (556 frente a 592 en 2005), como resultado de una disminución en la invocación de esta vía por parte de aquellos ciudadanos que consideran que no se han visto cumplimentados sus derechos de acceso, rectificación, cancelación u oposición. El derecho de cancelación alcanza el lugar predominante en las reclamaciones presentadas. Por otra parte, la Comunidad Autónoma donde reside el mayor número de reclamantes es la Comunidad de Madrid, con un 27%.

En lo que se refiere a la actividad desarrollada por el área de Instrucción, el sector de las telecomunicaciones y el financiero son también los que lideran la tabla, alcanzando el 46% de los 306 procedimientos sancionadores finalizados.

Es también significativo que en el 66% de los procedimientos sancionadores finalizados los imputados tenían su sede en la Comunidad Autónoma de Madrid.

Respecto de las Administraciones Públicas, la local continúa siendo la que ocasiona un mayor número de procedimientos de infracción.

SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS. PROCEDIMIENTO DE ACTUACIÓN

La Subdirección General de Inspección de Datos engloba tanto las labores de inspección como las de instrucción, bien diferenciadas en dos unidades, la Unidad de Inspección y la Unidad de Instrucción.

UNIDAD DE INSPECCIÓN

De conformidad con la LOPD, las autoridades de control podrán inspeccionar los ficheros a que hace referencia dicha Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos, examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

Compete a la Inspección de Datos de la Agencia Española de Protección de Datos efectuar inspecciones periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros, de titularidad pública o privada, en los locales en los que se hallen los ficheros y los equipos informáticos correspondientes.

Las funciones asociadas a la Unidad de Inspección son las siguientes:

- Estudiar y analizar las reclamaciones formuladas por los ciudadanos.
Realizar las investigaciones pertinentes encaminadas a determinar si existe infracción a la Ley Orgánica 15/1999, como consecuencia de una reclamación recibida en la Agencia, por petición del Director o a solicitud de un Inspector-Instructor durante la tramitación de un Procedimiento de Tutela de Derechos, un procedimiento Sancionador o un Procedimiento de Infracción de las Administraciones Públicas.

- Participar en proyectos de adaptación a la normativa europea en países de reciente incorporación a la Unión Europea, en los cuales la Agencia Española de Protección de Datos actúa como coordinadora.
- Asesoramiento en proyectos en los que se requiere una especial cualificación técnica.
- Colaboración en el desarrollo de planes de oficio sectoriales realizando inspecciones a las entidades implicadas y elaborando informes de conclusiones parciales acerca de la adaptación del sector inspeccionado a la legislación de protección de datos.

UNIDAD DE INSTRUCCIÓN

A la Subdirección General de Inspección de Datos le corresponde también la función instructora en los expedientes sancionadores, esto es, el ejercicio de los actos de instrucción relativos a los expedientes sancionadores (art. 29 del Estatuto).

El ejercicio de esta función instructora correspondiente a la Subdirección General de Inspección de Datos, no es más que la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia (art. 37.g de la LOPD) y la necesaria garantía del procedimiento sancionador, cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas a órganos distintos (art. 134 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).

El procedimiento sancionador, de conformidad con lo previsto en el art. 48.1 de la LOPD, está regulado en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD, en vigor tras la LOPD, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones. Se estructura como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución.

Por otra parte, la función instructora se concreta en la incoación de tres clases de procedimientos: el procedimiento sancionador incoado contra los responsables de ficheros de titularidad privada por infracción de los principios y reglas contenidos en la LOPD; el procedimiento por infracciones de las Administraciones Públicas (art. 46) cuando es una Administración de esta clase la que vulnera los preceptos de la Ley; y el procedimiento de tutela de derechos previsto en el art. 18 de la Ley, que se activa cuando son vulnerados los derechos de oposición, acceso, rectificación o cancelación de los afectados (arts. 15 a 17).

El procedimiento de tutela de derechos supone la existencia de un posible incumplimiento de la Ley que no sea constitutivo de infracción, lo que justifica referirse a esta potestad arbitral de tutela al margen de la potestad sancionadora de la AEPD. La nueva LOPD ha venido a reproducir el mismo esquema que regía bajo la vigencia de la derogada LORTAD, si bien ha introducido dos novedades en el procedimiento de tutela de

derechos al ampliar el plazo máximo para dictar resolución a seis meses (art. 18.3 LOPD), siguiendo la pauta general que para los procedimientos administrativos establece el art. 42.2 la Ley 30/1992, de 26 de noviembre, y dar entrada en la regulación de estos procedimientos a un nuevo derecho que se desconocía en la anterior legislación: el derecho de oposición, que consiste en esencia en que en aquellos casos en que no sea necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal (art. 6.4).

RESOLUCIONES MAS RELEVANTES

DATOS DE SALUD

Por lo que se refiere a los datos de salud, las resoluciones que, por su interés, deben ser resaltadas son las siguientes:

La Resolución *R/00566/2006*, en el marco del Procedimiento Sancionador *PS/00041/2006*, analiza si es conforme a la normativa de protección de datos realizar una prueba de detección de anticuerpos de SIDA, sin contar con el consentimiento expreso del afectado. La situación se produjo con motivo de la formalización de varios créditos hipotecarios concedidos por una entidad bancaria, para lo que el afectado debía suscribir dos solicitudes de seguro de vida a favor de la misma. Para ello, la Directora de la sucursal le indicó que debía someterse a un reconocimiento médico, que finalmente le fue realizado en un Centro Clínico, sin que éste le informara verazmente sobre la naturaleza del reconocimiento que incluía análisis de sangre y orina. Añadía el denunciante que no le informaron, en ningún momento, que los análisis incluían la prueba de SIDA. Además esa prueba no fue solicitada por la entidad con la que iba a suscribir el seguro de vida.

Ante esta situación, la Agencia consideró que la Clínica no debió realizar la mencionada prueba puesto que no contaba con el consentimiento expreso del afectado para hacerlo, tratándose de un dato especialmente protegido. Se sancionó por la infracción del artículo 7.3 de la LOPD, al no haber quedado acreditado el consentimiento del denunciante.

Resolución *R/00445/2006*, Procedimiento Sancionador *PS/000142/2005*. Se imputó a una entidad dedicada al Diagnóstico y Control médico, un tratamiento de datos de salud del denunciante y una comunicación de tales datos al Ministerio de Defensa, en ambos casos sin consentimiento de aquél y sin que dicha actuación se encuentre amparada en una norma con rango de ley.

La entidad dedicada al Diagnóstico y Control médico actúa como Servicio de Prevención Ajeno de Riesgos Laborales, en virtud de un contrato administrativo de

prestación de servicios formalizado con el citado Ministerio, que tiene por objeto la realización de reconocimientos médicos específicos al personal funcionario y laboral que presta servicios en dicho Departamento, de los establecidos como voluntarios en el artículo 22 de la LPRL. Esta Ley habilita el acceso a los datos de los trabajadores del Ministerio por parte de la entidad dedicada al Diagnóstico y Control médico. No obstante, esa entidad realizó un estudio médico fuera del establecido en el contrato de prestación de servicios suscrito entre ella y el Ministerio sin contar con el consentimiento del afectado, incurriendo en la infracción del artículo 7.3 de la LOPD.

Por otro lado, se prohíbe el acceso a la información médica obtenida al amparo de lo dispuesto en la LPRL por parte del empresario o de cualquier tercero, incluidas las personas u órganos con responsabilidades en materia de prevención, distintos del *"personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores"*, con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores para el desempeño del puesto de trabajo. En este caso, quedó acreditado que la entidad dedicada al Diagnóstico y Control médico facilitó a la Unidad de Coordinación de Riesgos Laborales del Ministerio de Defensa copias del reconocimiento médico específico y del informe psicológico complementario efectuados al denunciante, sin que conste el consentimiento expreso de éste. Por tanto, se concluye que tal actuación constituye una comunicación de datos de salud contraria a lo previsto en el artículo 11 de la LOPD en relación con el artículo 22 de la LPRL.

Resolución de Archivo de Actuaciones del *E/00828/2005*, de fecha 16 de junio de 2006. Cuatro personas, pertenecientes a una misma familia, formularon denuncia contra una Mutua de Seguros, una compañía de Seguros y contra un médico en base a que la Mutua y la Compañía de Seguros se habrían cedido e intercambiado los datos relativos a la salud de los denunciados en *"una pretendida investigación extrajudicial de un supuesto fraude cometido por XXX y que desembocó en una querrela contra éstos"*, y la Mutua de Seguros habría comunicado los datos de salud de XXX al médico sin su consentimiento. Dos de los denunciados acompañaban copia de la querrela criminal interpuesta por la Mutua y la Compañía de Seguros, por un presunto delito continuado de estafa agravado y de falsedad.

En cuanto a la cesión de datos entre las compañías de seguros sin consentimiento del denunciante, dicha cesión estaría habilitada si una Ley lo establece. En ese sentido los denunciados contrataron dos seguros distintos que cubrían el mismo riesgo, sin comunicar este hecho, como era su obligación, salvo pacto en contrario, a cada una de las dos compañías aseguradoras. La Mutua se enteró de que XXX tenía un seguro de enfermedad, que cubría los mismos riesgos contratados con dicha Mutua, porque el propio denunciante le envió, por error, una carta solicitando el reintegro de cantidades que ya habían abonado, y que iba remitida a la otra compañía. En el marco de lo dispuesto en el artículo 32 de Ley 50/1980, ambas compañías estaban habilitadas para investigar el sobreseguero (la suma asegurada supera el valor de lo asegurado) que no

había sido comunicado por el asegurado, con el fin de no abonar la indemnización. Por tanto, no se había producido una cesión que vulnera lo establecido en la LOPD entre ambas compañías aseguradoras, ya que los datos eran ya conocidos por ambas y, además, se los había facilitado el propio denunciante con la finalidad de obtener los gastos de reembolso de los gastos ocasionados por su enfermedad.

Por último, acerca de la cesión de datos de la Mutua al médico, constaba en el procedimiento el nombramiento del médico como perito de la mencionada Mutua, de conformidad con lo establecido en el artículo 38 de la Ley de Contrato de Seguro y su aceptación del cargo de perito. Además, en este caso, contaba con el consentimiento expreso del denunciante que autorizó el estudio de su historia clínica.

INFORMACIÓN EN LA RECOGIDA DE DATOS (Artículo 5 LOPD)

Resolución *R/00712/2006*, Procedimiento Sancionador *PS/00056/2006*. Se denunciaba que un Organismo Autónomo de Desarrollo Local de una Diputación Provincial había tramitado unas solicitudes de empleo de una sociedad anónima, que carecían de la cláusula informativa exigida legalmente para recabar los datos personales de los interesados. El Organismo imputado señalaba que no había solicitado dato personal alguno a ninguno de los solicitantes de empleo, y que éstos los habían facilitado voluntariamente. Destacaba en sus alegaciones los motivos sociales y altruistas de fomento de empleo que, en todo momento, habían conducido su actuación.

La obligación que impone este artículo 5 de la LOPD es la de informar al afectado en la recogida de sus datos personales, pues sólo así queda garantizado el derecho del afectado a tener una adecuada información y a consentir o no el tratamiento de sus datos, en función de la información recibida. La LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales, vinculando el consentimiento del afectado a la información previa que reciba. Se impone, por tanto, una formalidad específica en la recogida de datos a través de cuestionarios u otros impresos que garantice el derecho a la información de los afectados, debiendo constar dicha información en los mismos de forma claramente legible.

Se sancionó la inexistencia de la cláusula informativa que impone el artículo 5 de la LOPD, que debe incluirse por escrito en los formularios de recogida de datos.

Resolución de Archivo de Actuaciones del *E/00625/2005*, de 1 de septiembre de 2006. Se recibió una denuncia de un Sindicato, manifestando que una empresa de telefonía recababa datos personales de clientes a través de su página web sin aportar información concreta del destinatario de los datos facilitados por los clientes que accedían a esta página, ya que constaba como destinatario una entidad no inscrita en el Registro Mercantil. Se verificó que en la página web, objeto de la denuncia, en la que se recaban los datos de los clientes aparece: "*Aplicaciones de Negocio*", y "*Envíenos sus datos*",

se formula la pregunta de si la "empresa" es cliente de empresa de telefonía o no, y relaciona, a continuación, los campos que se deben rellenar por la misma. En la página se contiene la información completa que se incluye en el artículo 5 de la LOPD.

Se archivaron las actuaciones ya que en virtud de lo dispuesto en el artículo 1 de la LOPD, esta Ley no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley. Tampoco se aplica a los profesionales en su actividad bajo la forma de empresa ostentando, en consecuencia, la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio ni a los empresarios individuales en su actividad comercial y mercantil diferente de su propia actividad privada.

CALIDAD DE DATOS (Artículo 4.3 LOPD)

Resolución *R/00439/2006*, Procedimiento Sancionador *PS/00004/2006*. Plantea el caso de una entidad bancaria que incluye a un cliente suyo en un fichero de solvencia patrimonial y crédito, asociado a una deuda, a pesar de que ésta había sido cancelada y así se había hecho constar previamente en escritura pública. Tras la primera reclamación del cliente, la entidad bancaria cancela la inclusión en el citado fichero. Sin embargo le vuelve a incluir posteriormente por la misma deuda.

En este procedimiento se declaró la infracción por cuanto que, con independencia de que la deuda fuera cierta, vencida y exigible y hubiera resultado impagada, de acuerdo a la Instrucción 1/1995 de esta Agencia no puede incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga lo anterior. En consecuencia, los datos personales del cliente que mantenía la entidad bancaria no respondían con veracidad a la situación actual del mismo.

Por otra parte, se evidenció una falta de diligencia por parte de la entidad bancaria que en una primera ocasión atiende la reclamación presentada por el cliente y cancela sus datos del fichero de solvencia, para posteriormente, volver a incluirlo por los mismos motivos. En este sentido, los criterios de la Audiencia Nacional subrayan la obligación de las entidades gestoras de los datos de observar una especial diligencia para mantener éstos al día y evitar así el menoscabo que para la imagen y el prestigio de la persona supone figurar, indebidamente, en un fichero de solvencia patrimonial y crédito.

CESIÓN DE DATOS (Artículo 11 LOPD)

Resolución *R/00301/2006*, Procedimiento Sancionador, *PS/00149/2005*. Una Asociación, que tiene un Acuerdo de colaboración con una entidad bancaria para que emita tarjetas de pago a sus socios, cede los datos correspondientes a un domicilio

erróneo de una socia, en trámites de separación, con la consecuencia de que la entidad bancaria comienza a enviar extractos bancarios de la cuenta de la socia a ese domicilio erróneo, que es el de su ex-cónyuge, también socio de la misma Asociación.

En este procedimiento se declaró la infracción de los artículos 11 (Cesión) y del 4.3 (Calidad) de la LOPD por la Asociación y de los artículos 6 (Consentimiento) y del 10 (Secreto) de la LOPD a la entidad bancaria.

En la Resolución se considera que ha existido la cesión de datos de la Asociación a la entidad bancaria ya que, a pesar de que existía un Acuerdo de colaboración entre ambas entidades y del consentimiento otorgado por los socios en el ámbito de la gestión de la tarjeta, la Asociación no estaba habilitada para ceder el dato del cambio de domicilio de la citada socia a la entidad bancaria, máxime cuando éste era erróneo y, asimismo, tampoco había contado con el consentimiento de la socia para efectuar el cambio del domicilio.

Resolución de archivo de actuaciones E/00506/2006. Se procedió al archivo en otro supuesto en el que una persona denunció que tras la desaparición de una empresa de seguridad "XXX, S.L." con la que había suscrito un contrato de suministro, instalación, mantenimiento y explotación de una central de alarma, una empresa financiera le reclamó el pago de una deuda contraída en base a la cesión de los derechos contractuales de "XXX, S.L."

El denunciante contrató los servicios de la empresa "XXX, S.L." por importe aplazado de pago en 48 mensualidades. En el punto 9 de las "Condiciones Generales" del contrato se establece que *"El comprador faculta a "XXX, S.L." para que pueda ceder todos los derechos que dimanen del presente contrato a cualquier entidad financiera, establecimiento financiero de crédito o entidad de crédito, siendo por tanto esta entidad la que girará en su caso los recibos de pago aplazado, siendo liberatorio el pago de la misma. Esta cesión no supondrá modificación de las condiciones del presente contrato, salvo que medie acuerdo expreso entre ambas partes."*

La entidad crediticia suscribió un "CONTRATO MARCO DE CESIÓN DE DERECHOS DE CRÉDITOS" con "XXX, S.L.", teniendo como objeto la cesión de los créditos comerciales que ésta ostentara legítimamente frente a terceros que tuvieran su causa dentro del giro o tráfico de su actividad, y que se ajustaran a las características pactadas en los créditos susceptibles de cesión. En la Cláusula Quinta del citado contrato establecía la obligación por parte del cedente de notificar el acuerdo de cesión de crédito a sus deudores.

Quedó acreditado que el denunciante, al contratar, había otorgado su consentimiento para que "XXX, S.L." pudiera comunicar sus datos a una entidad financiera, para que girara los recibos de pago aplazado. Esta posibilidad prevista en el contrato se hizo efectiva al firmarse el contrato de cesión de derechos de crédito entre "XXX, S.L." y la entidad crediticia. Por tanto, no se observó, en este caso, vulneración de la normativa de protección de datos.

CONSENTIMIENTO (Artículo 6 LOPD)

Resolución R/00362/2006, Procedimiento Sancionador PS/00344/2005; Aborda el tratamiento sin consentimiento por parte de una empresa que, para realizar estudios de mercado, recaba los datos personales de los profesionales médicos utilizando, entre otros medios, los tabloneros de los Centros de trabajo de Sanidad Pública y Privada, asociándolos posteriormente en sus ficheros a determinadas prescripciones de medicamentos. Todo ello sin contar con el consentimiento autorizado de los citados profesionales de la medicina.

En este procedimiento se declaró la infracción del artículo 6.1 de la LOPD. En primer lugar, a pesar de que los datos de los colegiados médicos se refieran a su actividad profesional, quedan dentro del ámbito de la aplicación de la LOPD, de acuerdo a lo expresado por la STC 292/2000 que declara que *"el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de las personas, sino a cualquier tipo de dato personal, sea o no íntimo"*. En segundo lugar, el Tribunal de Justicia de la Unión Europea, en la Sentencia de 06/11/2003 señaló, al hablar de datos personales que *"incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones"*. Finalmente, los tabloneros de los Centros de trabajo no tienen *carácter de fuentes de acceso público*, que vienen debidamente relacionadas en el artículo 3. de la LOPD, por lo que la empresa no contaba con el consentimiento de los profesionales citados para tratar sus datos personales.

En el expediente E/00073/2006, analizaba la presentación en la Audiencia Nacional de dos Resoluciones, dictadas por un Colegio Profesional y correspondientes a un procedimiento sancionador en las que aparecían los datos personales del imputado, sin que hubiera dado su consentimiento para la cesión de sus datos.

Se resolvió el archivo de la denuncia. En primer lugar de acuerdo al artículo 6.2 de la LOPD que establece que no sería preciso el consentimiento cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas, puesto que el afectado era miembro del Colegio Profesional. También se archivó de acuerdo con el artículo 11.2 de la LOPD, que establece que no será necesario el consentimiento del interesado cuando el destinatario de la comunicación sea o los Jueces o Tribunales o así lo disponga una Ley.

En el expediente E/00199/2006, se trata de la comunicación de datos de un fallecido que hace una entidad bancaria a uno de sus herederos y que es denunciada por otro.

En este caso, se resolvió el archivo de la denuncia, de acuerdo al artículo 1 y 3 de la LOPD, debido a que esta Ley Orgánica tiene como objeto la protección de los datos personales de personas físicas, y, además, porque como señala el Código Civil en su artículo 30 la personalidad civil se extingue por la muerte de las personas.

En la Resolución nº R/00198/2006, Procedimiento Sancionador PS/00039/2005 se consideró que para la contratación telefónica, el artículo 5.3 de la Ley 7/1998, de 13 de

abril, sobre condiciones generales de contratación, establece que "... será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma". El desarrollo reglamentario de esta norma se encuentra en el Real Decreto 1906/1999, de 17 de diciembre, que regula la contratación telefónica o electrónica con condiciones generales. Este Real Decreto impone al predisponente la obligación de facilitar al adherente, previamente a la celebración del contrato, información sobre las cláusulas de éste y de sus condiciones generales, así como la obligación de confirmar documentalmente la contratación efectuada por vía telefónica, electrónica o telemática mediante la remisión al adherente de la justificación por escrito de la contratación efectuada donde deberán constar todos los términos de la misma.

En el caso referido, se ha incorporado al denunciante a un fichero de deudores sin que se haya podido acreditar la contratación y la existencia de la deuda cierta, vencida y exigible.

ADMINISTRACIONES PÚBLICAS

En la Resolución nº R/00398/2006, Procedimiento AAPP/00030/2005 se sancionó a la AEAT por publicar un acto administrativo en el Boletín Oficial indicando la cualidad de deudora de una persona, cuando en realidad era interesada en el procedimiento.

En la Resolución R/00083/2006, Procedimiento AAPP/0006/2005 se declara la vulneración del principio de calidad de datos (artículo 4.1 de la LOPD), dado que en un centro docente los datos recabados para la formalización de la matrícula fueron tratados para finalidades incompatibles para las que fueron recabados, al ser comunicadas a una entidad financiera.

Por dicha actuación se declaró la infracción del artículo 4.1 de la LOPD, tipificada como grave en el artículo 44.3.d).

En la Resolución R/00619/2006, Procedimiento AAPP/00028/2005 se analiza la actuación de un ente territorial que implementó un sistema de control de presencia mediante identificación de huella dactilar. Al mediar una relación laboral entre el ente y los trabajadores, resulta conforme a la normativa de protección de datos. No obstante se declaró una infracción por parte del ente territorial que no tenía inscrito el fichero en el que se recogían los datos personales.

En la Resolución R/00293/2006, Procedimiento AAPP/40/2005 se analiza la actuación de un Colegio Profesional que publicó en su intranet datos personales relativos a una sanción a de un miembro de dicho colegio, sin anonimizar.

Al final del citado procedimiento se declaran las infracciones de los artículos 9 y 10 (Secreto) de la LOPD, tipificadas como graves en los artículos 44.3.h) y g) de la LOPD.

TUTELAS DE DERECHOS

TD/00326/2006, Resolución R/00743/2006. La Agencia Española de Protección de Datos estimó la reclamación por la denegación del derecho de acceso a los datos personales del reclamante contenidos en los ficheros de un Ayuntamiento. No se le facilitó el acceso a dichos datos porque aquél había señalado como lugar de notificaciones un apartado de correos en vez de un domicilio. El Ayuntamiento, subrayaba que el único motivo por el que requería la comunicación por el reclamante de un domicilio a efecto de notificaciones era por un estricto cumplimiento de la normativa contenida en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en los artículos 35, 39 y siguientes del Real Decreto 1829/1999, de 3 de diciembre, por el que se regula la prestación de los servicios postales.

El artículo 59.2 de la LRJPAC dispone que *"En los procedimientos iniciados a solicitud del interesado, la notificación se practicará en el lugar que éste haya señalado a tal efecto en la solicitud. Cuando ello no fuera posible, en cualquier lugar adecuado a tal fin, y por cualquier medio conforme a lo dispuesto en el apartado 1 de este artículo"*.

Por su parte, la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación establece en el punto 3 de su Norma Primera que *"El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá: Domicilio a efectos de notificaciones, fecha y firma del solicitante"*.

Se estimó la Tutela al admitirse que la legislación ampara la idoneidad de un apartado de correos a efectos de notificación porque reviste las garantías necesarias.

TD/00341/06, Resolución R/00959/2006, en la que la Agencia Española de Protección de Datos no estimó la reclamación por la denegación del derecho de acceso del reclamante a los datos de su causahabiente contenidos en los ficheros de una entidad bancaria. Estimó que es un derecho personalísimo que se extingue con la muerte de su titular y, por tanto, la petición formulada por el reclamante no puede atenderse por cuanto se refiere a un derecho sobre el cual no ostenta la titularidad.

En este sentido el artículo 11, párrafo primero del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados preceptos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD establece "los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero". Asimismo, de acuerdo con el artículo 32 del Código Civil "la personalidad civil se extingue por la muerte de las personas", por lo que habiendo fallecido el titular de los datos se produce, la extinción de los derechos inherentes a la personalidad.

TD/00312/2006, Resolución R/00897/2006, El reclamante ejerció ante la Guardia Civil el derecho de cancelación de sus datos personales, conservados en un fichero de ante-

cedentes policiales, relativos a tres diligencias policiales seguidas contra el mismo, fundamentando su petición en los Autos firmes adoptados al respecto por la jurisdicción ordinaria, que resolvió los supuestos contenidos en dichos atestados con sobreseimiento provisional.

La Guardia Civil alegó que el almacenamiento de Diligencias Policiales en una base de datos de "delincuencia" constituye una información necesaria e irrenunciable para la investigación criminal, que los datos sobre antecedentes policiales registrados en la base de datos "INTPOL" de la Guardia Civil no está limitada por la conclusión de una investigación concreta y que su cancelación estará regida por otros criterios como los recogidos en el artículo 22.4 de la LOPD. Sin embargo, este planteamiento es contrario a lo establecido en las normas aplicables, incluido dicho artículo, que vincula expresamente la cancelación de los datos que figuran en ficheros de las Fuerzas y cuerpos de Seguridad a "*la conclusión de una investigación o procedimiento concreto*".

TD/00230/2006; RESOLUCIÓN R/ 00563/2006, La Agencia Española de Protección de Datos estimó la reclamación presentada por la denegación de su derecho de acceso a sus datos personales contenidos en los ficheros de un Casino. El Casino contestó al reclamante informándole de manera telegráfica e ininteligible los datos que sobre el mismo obraban en sus archivos.

El artículo 15, en sus apartados 1 y 2, de la LOPD dispone que "*1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos*".

En dicha resolución quedó acreditado que el Casino debió contestar en plazo al reclamante. Sin embargo, envió la contestación al ejercicio del derecho de cancelación cuando había transcurrido más de un mes desde que recibiera la solicitud del reclamante, por lo que se estimó la reclamación por motivos formales. Respecto a la forma de facilitar el acceso a sus datos personales, quedó acreditado el derecho de acceso no se atendió de forma inteligible para el reclamante, por lo que también se estimó la reclamación de Tutela de Derechos, en el sentido de que el Casino debía aclarar el reclamante el significado de las expresiones utilizadas en el escrito remitido .

COMUNICACIONES ELECTRÓNICAS COMERCIALES NO DESEADAS (Artículo 21 LSSI)

En el expediente *PS/00219/2005* se analizó, al hilo de las alegaciones formuladas por el imputado, que comprobado que la dirección electrónica desde la que se remitió el mensaje se corresponde con una dirección IP, cabe deducir que su titular es el responsable de

la infracción de envío de comunicación comercial sin consentimiento, sin que sirva de excusa, salvo prueba fehaciente en contrario, la manifestación de que fue enviado por un agente comercial o una tercera persona, sin consentimiento del titular de la IP. Además, el hecho de que la dirección de correo electrónico a la que se remitió el envío hubiese sido obtenida de un tercero, no sirve para exculpar la conducta típica prevista.

En el expediente *PS/215/2005* se analiza el ámbito de aplicación de la LSSI. De acuerdo con lo señalado, es preciso analizar el concepto de Servicios de la Sociedad de la Información y, a continuación, determinar los supuestos, recogidos en el párrafo segundo del Anexo f) de la LSSI, que no se consideran, a los efectos de esta Ley, como comunicaciones comerciales.

La LSSI en su Anexo a) define como Servicio de la Sociedad de la Información, "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario". A través de dicha definición el legislador español transpuso el concepto recogido en la Directiva 98/34/CEE, de 22 de junio, del Parlamento y del Consejo, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la Sociedad de la Información, modificada por la Directiva 98/84/CE, de 20 de noviembre, del Parlamento y del Consejo, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso. Dicha definición se refiere, tal y como se expresa en el Considerando 17 de la citada Directiva 2000/31/CE, a "cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico para el tratamiento (incluida la comprensión digital) y el almacenamiento de datos, y a petición individual de un receptor de un servicio", añadiendo que estos servicios cuando "no implica tratamiento y almacenamiento de datos no están incluidos en la presente definición".

De acuerdo con lo señalado, el concepto de comunicaciones comerciales ha de tratarse de todas las formas de comunicaciones destinadas a promocionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o profesional, y, además, ha de realizarse dicha comunicación en los términos que señala el Considerando 17 de la Directiva 2000/31/CE que recoge lo previsto en las citadas Directivas 98/34/CE y 98/84/CE. De lo anterior se deduce que, cuando la comunicación comercial no reúne los requisitos que requiere el concepto de Servicios de la Sociedad de la Información, pierde el carácter de comunicación comercial a los efectos de la ley.

COMUNICACIONES COMERCIALES NO SOLICITADAS EN EL ÁMBITO DE LA LEY GENERAL DE TELECOMUNICACIONES

En el expediente *PS/00239/2005*, así como en el *PS/00231/2005*, se refiere el envío de faxes con falta de consentimiento previo e informado del abonado. En el citado envío, se le comunicaba que los datos que contenía el fichero que sirvieron para el envío de los faxes fueron obtenidos del repertorio telefónico de "Páginas blancas" y como tal

gozaban del carácter de fuente de acceso público, según la LOPD. Sin embargo el artículo 38.3.h) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (en lo sucesivo LGT), establece el derecho de los abonados a los servicios de comunicaciones electrónicas "a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello", y en relación a la prestación de consentimiento para el envío de este tipo de comunicaciones, en tanto que manifestación de voluntad específica informada, resulta obvio que el hecho de que los datos utilizados para el envío de los mensajes citados figuren en una fuente accesible al público resulta insuficiente para que pueda entenderse cumplida la exigencia de consentimiento previo e informado.

PLAN SECTORIAL DE OFICIO A LA ENSEÑANZA REGLADA NO UNIVERSITARIA

Como ya se anticipaba en la Memoria del año pasado, el Plan Sectorial de Oficio a la Enseñanza Reglada no Universitaria llegó a su recta final en 2006.

Es importante señalar que se trata del Plan más amplio realizado por la Agencia hasta el momento, no sólo por el número de centros escolares existentes en nuestro país que imparten enseñanza reglada no universitaria sino por el amplio tipo de datos, de toda naturaleza, que se tratan en los mismos.

El número total de centros escolares auditados así como el detalle de los mismos por Comunidad Autónoma queda reflejado en la siguiente tabla:

COMUNIDAD AUTÓNOMA	CENTROS PÚBLICOS		CENTROS CONCERTADOS	CENTROS PRIVADOS	TOTAL
	COLEGIO PÚBLICO	INSTITUTO			
ANDALUCÍA	1	1	1	1	4
ARAGÓN	1	1	1	1	4
ASTURIAS	1	1	1	1	4
CANARIAS	1	1	1	1	4
CANTABRIA	1	1	1	1	4
CASTILLA-LA MANCHA	1	1	1	1	4
CASTILLA Y LEÓN	1	1	1	1	4
CATALUÑA	(*)	(*)	1	1	2
C. VALENCIANA	1	1	1	1	4
EXTREMADURA	1	1	1	1	4
LA RIOJA	1	1	1	(**)	3
GALICIA	1	1	1	1	4
ISLAS BALEARES	1	1	1	1	4
MADRID	(*)	(*)	1	1	2
MURCIA	1	1	1	1	4
NAVARRA	1	1	1	1	4
PAIS VASCO	(*)	(*)	1	1	2
TOTAL	14	14	17	16	61

(*) Estas Comunidades Autónomas tienen Agencia de Protección de Datos Autonómica.

(**) La Comunidad Autónoma de La Rioja no tiene colegios privados, toda la enseñanza es pública o concertada.

Las áreas y servicios escolares que fueron auditados fueron las siguientes:

- Admisión de alumnos: se examinaron los formularios empleados y la documentación solicitada, analizando la legislación que regula este procedimiento.
- Matriculación: se estudiaron los formularios utilizados, la información que se facilita a las familias, los tratamientos que realizan posteriormente con los datos y documentación recabada así como la legislación que lo regula.
- Ciclo Escolar: se analizaron los tratamientos que realizan los centros durante la etapa escolar, la relación con otras administraciones y las cesiones de datos a terceros y su regulación.
- Servicio de Orientación: se analizó la actividad que realiza este departamento y la información que se facilita a los padres atendiendo a la legislación que lo regula.
- Servicio médico y programas de salud escolar: se auditó si los centros escolares recaban datos de salud de sus alumnos, los tratamientos que, en su caso, realizan con los mismos y la información que facilitan a las familias.
- Servicios ofertados por el centro escolar a los alumnos: se detallaron y analizaron los distintos servicios que prestan los centros escolares a sus alumnos como complemento a la labor educativa, si están contratados con terceras empresas y si la relación se encuentra regulada mediante el correspondiente contrato.

Además de los aspectos citados anteriormente, se verificaron las medidas de seguridad implantadas en los centros escolares. En este punto se revisó el nivel de implementación de las medidas de seguridad reguladas en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (en lo sucesivo Reglamento de Medidas de Seguridad).

A continuación se expone un breve resumen de los resultados que figuran en el documento final de Conclusiones y Recomendaciones que fue presentado públicamente:

PRINCIPIOS DE INFORMACIÓN Y CONSENTIMIENTO

En este punto se analizaron los distintos momentos en los que los centros escolares recaban datos personales, tanto de los alumnos como de sus familias, si facilitan información adecuada según la normativa de protección de datos y si de ésta puede desprenderse que cuentan con el consentimiento adecuado a cada tratamiento.

■ CENTROS PÚBLICOS:

En general, la mayoría de los formularios que utilizan los centros escolares no llevan impresa una cláusula que informe de lo recogido en el artículo 5 de la Ley Orgánica

de Protección de Datos (en lo sucesivo LOPD). Esto puede hacerse extensivo a los formularios oficiales normalizados por las Consejerías de Educación utilizados por los centros, que tampoco suelen llevar impreso ningún texto alusivo al artículo 5 citado. No obstante, algunas Consejerías han incorporado un texto alusivo a la LOPD pero no puede considerarse adecuado a lo dispuesto en la normativa de protección de datos.

El hecho de que los centros escolares no utilicen cláusulas informativas o faciliten información incompleta, lleva a concluir que, para determinadas actuaciones, no disponen del consentimiento regulado por la normativa para tratar los datos personales. Como ejemplo podría citarse la publicación de fotos en anuarios.

Por otra parte, determinados tratamientos como son los relativos a solicitud de plaza escolar, gestión de libro de escolaridad o de becas y el tratamiento de datos para la expedición de títulos académicos, se encuentran regulados por la legislación vigente en materia educativa nacional y autonómica y, por tanto, no precisan de consentimiento.

■ CENTROS PRIVADOS CONCERTADOS:

Estos centros escolares, al tratarse de centros sostenidos con fondos públicos, utilizan los formularios normalizados por su Consejería de Educación para determinados tratamientos como el proceso de solicitud de plaza. Por tanto, se trata de los formularios citados en el apartado relativo a centros públicos donde ya se ha comentado que no se incluye ninguna cláusula que haga referencia al artículo 5 de la LOPD o ésta es incompleta.

Respecto del resto de los formularios utilizados por los centros concertados, que son de elaboración propia, tampoco se incluye una referencia completa al principio de información.

En cuanto al consentimiento, en el documento se concluye que los centros, a veces, no cuentan con el consentimiento inequívoco regulado por la normativa de protección de datos para tratar datos personales, cuando no exista habilitación legal para ello. Como ejemplo se puede citar la entrega de datos para participar en concursos, publicación de fotografías de alumnos en la página web del colegio o la entrega de datos personales a la AMPA, entre otros.

■ CENTROS PRIVADOS NO CONCERTADOS:

Estos centros presentan distinta casuística. Algunos colegios privados no incluyen, en ninguno de sus formularios, una cláusula relativa al artículo 5 de la LOPD aunque alguno solicita a los padres autorización para realizar algunos tratamientos muy concretos. Otros incluyen una cláusula informativa únicamente en el formulario de matriculación pero en otros formularios no la tienen en cuenta cuando sería necesario. Otros incluyen la cláusula pero no puede considerarse válida.

En cuanto al consentimiento, se concluye que los centros muchas veces no cuentan con el consentimiento inequívoco regulado por la normativa de protección de datos para tratar datos personales, cuando no exista habilitación legal para ello.

En todos los casos se recomienda que incluyan en los formularios las particularidades a que hace referencia el artículo 5 y 6 de la LOPD.

PRINCIPIO DE CALIDAD

Este apartado hace referencia al cumplimiento del artículo 4 de la LOPD "datos adecuados, pertinentes y no excesivos, además de cancelados cuando dejen de ser necesarios". Se analizaron los distintos momentos en que los centros escolares recaban datos personales y su tipología, valorando si pueden ser considerados adecuados, pertinentes y no excesivos en función de tratamientos posteriores que va a realizarse con ellos. Además se analizó la antigüedad de los mismos y los procedimientos de cancelación y bloqueo.

Los momentos analizados en este punto para poder obtener conclusiones fueron el proceso de solicitud de plaza escolar, de matriculación, gestión de becas de estudios, gestión del expediente académico y otros formularios de recogida de datos personales que utilizan los centros escolares.

■ CENTROS PÚBLICOS:

Respecto del proceso de solicitud de plaza, los datos personales recabados en los formularios normalizados por la Consejería de Educación, se pueden considerar adecuados, pertinentes y no excesivos para la finalidad de baremar las solicitudes siguiendo los criterios establecidos en la normativa autonómica. En cuanto a la cancelación de los datos, se dan situaciones muy variadas, tanto en lo relativo a los datos personales que se incluyen en aplicaciones informáticas como la documentación que se genera en soporte papel, pero se concluye que los centros escolares no han recibido instrucciones de la Consejería de Educación sobre cuándo y cómo deben cancelar los datos personales recabados y la documentación solicitada.

En el proceso de matriculación se observaron situaciones variadas que permitieron concluir, con carácter general, que los datos recabados se adecuan a lo dispuesto en el artículo 4 de la LOPD. No obstante hay que matizar que determinados datos recabados como el DNI, estudios, profesión y situación laboral de los padres, solicitada por algunos centros escolares, u otros datos como problemas que presentan los hermanos, son excesivos ya que no queda justificada la finalidad para la cual se recaban. Respecto de la cancelación, no existe ninguna política de cancelación, lo que provoca que los centros escolares no cancelen ningún dato personal en sus sistemas informáticos. La documentación se incluye en el expediente académico del alumno.

En la gestión de becas, los centros escolares suelen hacer de meros intermediarios ya que los organismos que convocan las ayudas son la Administración Central o la Autonómica que son, por tanto, los que elaboran los formularios de solicitud de datos personales. Los centros únicamente conservan indefinidamente los listados que le remiten los organismos correspondientes relativos a las becas concedidas y denegadas.

El expediente académico suele ser un fichero en soporte papel formado por carpetas de documentos asociadas a los alumnos. Está compuesto por todos aquellos documentos que se recaban durante la permanencia del alumno en el centro escolar.

A priori, podrían considerarse todos ellos adecuados, pertinentes y no excesivos, dado que se desconoce cuál tiene que ser su contenido exacto. Pero la inclusión de informes sobre alumnos con necesidades especiales y la conservación de la documentación recabada en el proceso de solicitud de plaza, podría considerarse un tratamiento excesivo. Respecto de la cancelación del expediente académico, los centros desconocen cuál es el contenido a conservar por lo que, actualmente, ningún centro escolar destruye expedientes académicos. No obstante, algún colegio conserva únicamente la documentación relativa a las notas escolares con la finalidad de elaborar certificados posteriores. Finalmente, en lo que se refiere a otros formularios, suelen recabarse datos adecuados, pertinentes y no excesivos y el problema suele presentarse en la cancelación ya que, los centros suelen mantener la información y documentación mientras los espacios, físicos y de capacidad tecnológica lo permitan.

■ CENTROS PRIVADOS CONCERTADOS:

Respecto del proceso de solicitud de plaza, dado que utilizan los formularios normalizados por la Consejería de Educación ya citados, se aplica la misma conclusión. Lo mismo sucede en el caso de la cancelación de los datos.

En el proceso de matriculación se han observado situaciones variadas que permiten concluir, con carácter general, que los datos recabados se adecuan a lo dispuesto en el artículo 4 de la LOPD, aunque datos como estudios, profesión y empresa donde trabajen los padres, solicitada por algunos centros escolares, parecen excesivos. Respecto de la cancelación, no existe ninguna política al respecto, lo que conlleva que los centros escolares no cancelen ningún dato personal de sus sistemas informáticos. La documentación se incluye en el expediente académico del alumno.

Ya se ha comentado anteriormente la información que contiene el expediente académico. Algunos centros escolares incluyen resoluciones relativas a los expedientes disciplinarios y, teniendo en cuenta que los expedientes académicos no suelen destruirse, se pueden conservar documentos referentes a faltas sancionadas prescritas.

Los centros concertados tampoco destruyen los expedientes académicos, conservándolos completos con la finalidad de elaborar certificados posteriores.

Finalmente, en lo que se refiere a otros formularios, suelen recabarse datos adecuados, pertinentes y no excesivos y el problema suele presentarse en el tema relacionado con

la cancelación, ya que suele mantenerse la información y documentación mientras los espacios físicos y de capacidad tecnológica, lo permitan.

■ CENTROS PRIVADOS NO CONCERTADOS:

Respecto del proceso de solicitud de plaza, estos centros utilizan sus propios medios consistentes en entrevistas, formularios y documentación. En general, los datos recabados son adecuados, pertinentes y no excesivos, sin embargo en algunos centros se recaban datos que pudieran considerarse inadecuados y excesivos como puede ser el trabajo de los padres o la existencia de un seguro de vida. Se ha concluido que no existen criterios para cancelar los datos.

En el proceso de matriculación se han observado situaciones variadas concluyendo que, con carácter general, la mayor parte de los datos recabados se adecuan a lo dispuesto en el artículo 4 de la LOPD, aunque datos solicitados por algunos centros, como estudios, profesión y empresa donde trabajan los padres, lugares donde pasa las vacaciones, datos de los abuelos, nombre del médico del alumno, si realiza otras actividades extraescolares o, el caso particular de un colegio, que solicita también información sobre la situación familiar de los padres (casados por la iglesia católica, civilmente u otra situación), parecen excesivos.

En lo relativo a la cancelación, algunos centros los centros escolares no cancelan ningún dato personal de sus sistemas informáticos mientras que otros cancelan los datos transcurrido un plazo indeterminado. La documentación se incluye en el expediente académico del alumno.

Los centros privados también cuentan con un fichero denominado expediente académico del tipo ya comentado. Tampoco destruyen los expedientes académicos si no que las conservan completo ante el desconocimiento de cuál es su responsabilidad en relación con el contenido y custodia de los expedientes académicos.

Finalmente, en lo que se refiere a otros formularios, suelen recabarse datos adecuados, pertinentes y no excesivos y el problema suele presentarse en el tema relacionado con la cancelación, ya que no existe una metodología para eliminar los datos automatizados y la documentación asociada.

En todos los casos se recomienda revisar los datos personales de tal forma que permita al centro escolar cumplir con el principio de calidad de datos y, por tanto, cancelar aquellos que han dejado de ser necesarios, así como destruir la documentación asociada a los mismos.

DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

Este apartado hace referencia a los derechos reconocidos por la LOPD a los ciudadanos relativos al acceso, cancelación, rectificación u oposición.

En general, los centros públicos y los centros concertados no informan de estos derechos ya que, según se ha comentado anteriormente, ningún formulario de recogida de datos incluye la cláusula relativa al artículo 5 de la LOPD. Esto conlleva que los centros escolares no dispongan de ningún procedimiento que les permita gestionar estos derechos.

Se da el caso de centros concertados que, aunque sí informan, tampoco cuentan con un procedimiento de gestión. Únicamente se ha detectado un colegio concertado que dispone del mismo.

Sin embargo, en los colegios privados, algunos han implementado un procedimiento escrito que permite gestionar los derechos citados, incluso un centro escolar utiliza un formulario que permite a una cualquier persona ejercer sus derechos ante el colegio. No es muy habitual que los centros escolares reciban solicitudes en este sentido.

En todos los casos se recomienda que incluyan en los formularios los extremos referentes a estos derechos.

INSCRIPCIÓN DE FICHEROS

Este apartado hace referencia a la obligación legal de inscribir los ficheros, bien mediante disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente o dirigiéndose al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Según resultados de la consulta realizada al Registro General de Protección de Datos y tomando como responsable la Consejería de Educación de cada Comunidad Autónoma se aprecia una omisión relevante de dicha obligación.

DATOS ESPECIALMENTE PROTEGIDOS

Este apartado se ha analizado si los centros escolares recaban y tratan este tipo de datos, en qué momento, si disponen del consentimiento respectivo o si la recogida y tratamiento de los mismos obedece a disposiciones legales de ámbito estatal o autonómico. Este apartado es bastante extenso y, dado que el documento se encuentra a disposición pública en la página web de la Agencia Española de Protección de Datos, se remite allí para su consulta. No obstante, se puede destacar lo siguiente:

■ CENTROS PÚBLICOS:

Se puede afirmar que todos los centros escolares, independientemente de la Comunidad Autónoma en la que se ubiquen, conocen datos de salud de los alumnos

o de sus familiares desde el momento en el que la familia cumplimenta el formulario de solicitud de plaza para un centro escolar sostenido con fondos públicos ya que se debe especificar y acreditar documentalmente, en su caso, la minusvalía o discapacidad, la enfermedad crónica que afecte al sistema digestivo, endocrino o metabólico del alumno que exija un control alimentario, las necesidades educativas especiales o si pertenece a minoría étnica o inmigrante con déficit social o cultural.

También solicitan información sobre el estado de salud del alumno en aquellos casos en que no puede participar en las actividades deportivas programadas en el curso escolar, no puede tomar determinado tipo de alimentos, si va a utilizar el servicio de comedor o si tiene algún tipo de enfermedad que obligue al centro a tener alguna atención especial con él como puede ser el caso de diabetes o alergias. También solicitan informes médicos (audiométricos, otorrinolaringológicos, oftalmológicos, etc.) cuando se trata de escolarizar alumnos que presentan un problema de salud (niños sordos, minusválidos, etc.).

Además, durante la etapa escolar también recaban datos especialmente protegidos sobre todo de alumnos con necesidades educativas especiales que, en el caso de los colegios públicos, son atendidos por un equipo multidisciplinar perteneciente a la Consejería de Educación y, en el caso de los institutos, por su propio departamento de orientación. Este departamento en algunos casos, también realiza pruebas psicopedagógicas a todos los alumnos del centro.

En el informe se ha concluido que, en algunos casos, los centros realizan tratamientos de datos especialmente protegidos sin que se cuente con el consentimiento expreso de los padres recomendándose la revisión de los protocolos de actuación de los equipos psicopedagógicos de las Comunidades Autónomas y de los servicios de orientación, al objeto de que, en ningún caso, se produzcan tratamientos de este tipo de datos sin el consentimiento expreso de los afectados.

■ CENTROS PRIVADOS CONCERTADOS:

Se ha comprobado que estos centros tratan datos especialmente protegidos. Los informes médicos, psicopedagógicos y los dictámenes de escolarización que recaban de alumnos con necesidades educativas especiales se tratan en el sistema de información del colegio sin disponer, para ello, del consentimiento exigido por la LOPD. Se ha constatado el caso de algún colegio que también trata datos de salud de los padres de los alumnos y, también, sin su consentimiento expreso.

Los colegios suelen comunicar a las familias la realización de pruebas psicopedagógicas pero no se solicita el consentimiento para el tratamiento de los datos personales. Se recomienda revisar los mecanismos de recogida y tratamiento de datos especialmente protegidos al objeto de recabar, en cada caso, el consentimiento regulado por la LOPD.

■ CENTROS PRIVADOS NO CONCERTADOS:

Algunos centros privados no disponen de un departamento de orientación ni de servicio médico, otros cuentan con ambos departamentos y en algunos casos, tienen uno u otro indistintamente. Pero, en cualquier caso, todos los colegios tratan datos especialmente protegidos ya que, aun cuando no disponen de estos departamentos, conocen datos de salud de sus alumnos necesarios para poder escolarizar al alumno adecuadamente en el centro.

Pueden citarse algún caso concreto detectado respecto del tratamiento de datos especialmente protegidos en colegios privados como la cesión de datos por parte del orientador cuando un alumno está siendo tratado por un centro externo a éste o la solicitud a una empresa externa de la elaboración de test psicopedagógicos, corrección y elaboración de informe quedándose toda la documentación en poder de la empresa. Como conclusión se recoge que en los centros privados se solicita autorización a los padres para realizar reconocimientos médicos pero no consentimiento expreso, según exige la normativa de protección de datos, para tratar los datos de salud. Respecto de los departamentos de orientación, los colegios suelen informar a las familias de la existencia del mismo en el centro pero éstos realizan los tratamientos de datos personales sin el consentimiento de la familia.

Se recomienda revisar los mecanismos de recogida y tratamiento de datos especialmente protegidos al objeto de recabar, en cada caso, el consentimiento regulado por la LOPD.

MEDIDAS DE SEGURIDAD

Se identificaron los ficheros, informáticos y en soporte papel, utilizados por los centros escolares para tratar datos personales de los alumnos, analizando las medidas de seguridad implantadas para impedir que los datos personales de los alumnos sean conocidos por terceros no autorizados. A continuación se expone un mínimo resumen de lo detallado en el documento de Conclusiones y Recomendaciones:

■ CENTROS PÚBLICOS:

El sistema de información más utilizado por los colegios públicos es el denominado "ESCUELA" y el de los institutos de enseñanza secundaria el denominado "IES2000". Estos sistemas suelen gestionarse en modo local no existiendo ninguna conexión con la Consejería de Educación. También se da el caso de Comunidades Autónomas que han implantado, o pretenden implantar a corto plazo, un sistema de gestión integral para todos sus centros escolares, instalado en las dependencias de la Consejería de Educación, al que todos los centros sostenidos con fondos públicos se conecten para gestionar su centro escolar.

El nivel de seguridad del fichero de alumnos debe ser ALTO, lo que no se corresponde con el nivel asignado en la actualidad, según consta en las inscripciones realizadas en el Registro General de Protección de Datos.

Ningún centro escolar dispone de documento de seguridad.

Las Consejerías de Educación no han elaborado y distribuido a los centros escolares visitados un documento en el que se encuentren definidas las funciones y obligaciones del personal.

Los centros escolares, normalmente, conocen cómo deben proceder ante una incidencia en sus sistemas informáticos frente a la Consejería de Educación, que es la encargada de su mantenimiento. Sin embargo, no existen procedimientos establecidos acordes al Reglamento de Medidas de Seguridad.

Con carácter general, los centros escolares no disponen de procedimientos escritos de asignación, distribución y almacenamiento de claves de identificación y autenticación y no suelen tener relaciones actualizadas de usuarios con acceso a los datos personales de los alumnos. No obstante, en la mayoría de los centros escolares se emplea un código de usuario y contraseña para acceder al sistema de información que gestiona los datos personales de los alumnos sin obviar que también se da el caso contrario, Las contraseñas no suelen cambiarse nunca. Finalmente, añadir que la gestión del acceso a los datos personales está muy limitada y suele ser escasa.

Todos los centros disponen de soportes informáticos con datos personales de los alumnos. Sin embargo, en la mayoría de los casos, no utilizan procedimientos para su gestión, los soportes no están inventariados y los centros escolares no tienen instrucciones sobre como reutilizarlos o destruirlos.

Ningún centro escolar dispone de instrucciones para realizar copias de respaldo y recuperación de tal forma que, cada centro las realiza a su libre albedrío. Incluso se da el caso de departamentos de orientación que no realizan nunca copias de respaldo de la información que gestionan.

Los centros no disponen de la figura denominada "responsable de seguridad" y, tampoco tienen constancia de que se haya realizado una auditoria de seguridad. Finalmente, la transmisión de datos por redes de telecomunicaciones se realiza sin tomar precauciones para que la información no sea manipulada por terceros.

■ CENTROS PRIVADOS CONCERTADOS:

Las aplicaciones informáticas más utilizadas son "SIGMA" y "GESDOC", desarrolladas por las empresas "COSPA" y "AID", respectivamente. Este software no permite a los centros escolares inspeccionados cumplir con las medidas establecidas por el Reglamento de Medidas de Seguridad para el nivel ALTO.

El nivel de seguridad del fichero de alumnos debe ser ALTO. Sin embargo no se corresponde con el nivel asignado por los centros escolares al fichero que gestionan ya que suele limitarse al nivel BASICO.

Siete centros disponen de documento de seguridad aunque no todos ellos se adecuan a los dispuesto en el Reglamento de Medidas de Seguridad.

Algunos centros han establecido las funciones y obligaciones del personal con acceso a datos de carácter personal, sin embargo no se ha comunicado a los afectados.

A excepción de dos centros escolares, la mayoría no disponen de procedimiento de gestión y notificación de incidencias. Tan sólo 4 utilizan un registro de gestión de incidencias.

Con carácter general, los centros escolares emplean un código de usuario y contraseña para acceder al sistema de información que gestiona los datos personales de los alumnos aunque, en algunos casos, la contraseña utilizada es compartida, incluyendo la utilizada por el departamento de orientación. En cuanto a la aplicación del control de accesos, podría considerarse adecuada al Reglamento en su práctica diaria pero no suele existir un documento escrito.

Todos los centros disponen de soportes informáticos con datos personales de los alumnos. Sin embargo, en la mayoría de los casos, no disponen de procedimientos que permitan su gestión, reutilización o destrucción y los soportes no están inventariados. En este punto debe añadirse que la gestión de los soportes es de lo más variado, con ejemplos como citar a profesores que se llevan a casa listados, o exámenes de alumnos u orientadores que la copia de seguridad de sus ficheros, permanece en su domicilio particular o la llevan en su cartera.

Cuatro centros escolares disponen de instrucciones relativas a la realización de copias de respaldo y recuperación aunque no cuentan con un procedimiento por escrito. Casi la mitad de los centros escolares han nombrado un responsable de seguridad sin embargo, sólo un centro ha realizado una auditoria.

■ CENTROS PRIVADOS:

Las aplicaciones informáticas más utilizadas son las citadas "SIGMA" y "GESDOC", desarrolladas por las empresas "COSPA" y "AID".

El nivel de seguridad del fichero de alumnos debe ser ALTO. Algunos colegios lo conocen y lo aplican a sus ficheros, sin embargo otros, aunque lo conocen, no lo aplican considerando simplemente el nivel BASICO.

La mayoría de los centros privados no han elaborado un documento de seguridad no obstante, algunos han implementado alguna medida de seguridad. Otros que han elaborado el documento de seguridad, no lo han implementado.

Muchos centros escolares no han establecido las funciones y obligaciones de su personal y, los que lo han establecido, no las han divulgado. Solo existe la excepción de un centro escolar que ha cumplido adecuadamente.

La mayoría de los centros no disponen de procedimientos de notificación y gestión de incidencias y no cuentan con el registro correspondiente. Algún colegio dispone de procedimientos en el documento de seguridad. Se trata de procedimientos estándar que no están implantados y si existe un registro de incidencias, no se cumplimenta.

Un buen número de centros no han establecido procedimientos de identificación y autenticación para acceder a los sistemas de información con datos personales aunque el acceso suele realizarse mediante el empleo de usuario y contraseña. Respecto del control de accesos, no suele existir una relación actualizada de usuarios.

Todos los centros disponen de soportes informáticos con datos personales de los alumnos, sin embargo, en la mayoría de los casos, no disponen de procedimientos que permitan su gestión, no están inventariados y no han definido cómo tratar los soportes para ser reutilizados o destruidos. No obstante, se da el caso de algunos colegios que tienen identificados los soportes y la documentación está archivada en locales cerrados con llave.

Los centros escolares realizan copias de respaldo y recuperación, algunos conservan las copias en una caja fuerte debidamente etiquetados. Sin embargo, falta la elaboración de procedimientos.

Prácticamente ningún centro ha nombrado un responsable de seguridad y cuando el centro dispone de dicha figura, la misma está asignada a una empresa externa sin la firma previa del contrato adecuado a la normativa.

En todos los casos se recomienda atender a lo recogido en el Reglamento de Medidas de Seguridad, teniendo en cuenta que las medidas de seguridad deben estar documentadas e implantadas. No se considera adecuado a la normativa de protección de datos tener un documento de seguridad con todos los procedimientos perfectamente definidos, cuando éstos no han sido implantados en el centro escolar y viceversa.

DEBER DE SECRETO

La legislación vigente, establece que *"En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que, afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo"*.

No obstante, ningún centro escolar público ha recibido instrucciones desde la Consejería de Educación en el sentido anteriormente citado, aunque el profesorado suele apelar a

su ética profesional manifestando que guardan celosamente la información a la que acceden. Los profesionales que trabajan en los departamentos de orientación son conscientes de la información de carácter personal que manejan, dado que es especialmente sensible, e incluso sus documentos los etiquetan con la palabra "CONFIDENCIAL", pero tampoco han recibido instrucciones desde su Consejería. El resto del personal, como son administrativos, personal de limpieza, conserjes o monitores deportivos, se encuentran en la misma situación pero agravada porque, en muchos casos, pertenecen a terceras empresas con las que no se ha firmado el contrato adecuado según la normativa de protección de datos.

Los centros concertados no están muy bien situados en este apartado ya que, únicamente los empleados de dos colegios han firmado un anexo a su contrato laboral relativo a la confidencialidad y, sólo en uno de ellos, además, se adjuntan las normas de seguridad que debe cumplir.

Entre todos los centros privados visitados, solamente cuatro disponen de un documento de confidencialidad firmado por sus trabajadores. El resto de colegios únicamente contratan a sus trabajadores siguiendo los modelos normalizados por la administración, sin añadir ningún clausulado específico.

CESIONES DE DATOS

En este punto se trató de conocer qué comunicaciones realizan los centros escolares a terceras entidades, públicas o privadas, y si las mismas se adecuan a la normativa de protección de datos.

Las cesiones que realizan los centros escolares sostenidos con fondos públicos tienen como destinatario distintos órganos de la Administración. Así, se entrega información a las Comisiones de Escolarización, en los casos de centros sostenidos con fondos públicos, a la Consejería de Educación, a la Consejería de Sanidad, a la Universidad y a la Tesorería General de la Seguridad Social. Los centros privados realizan las mismas cesiones a excepción de la Tesorería General de la Seguridad Social y la Comisión de Escolarización.

El hecho de que los datos se entreguen a órganos de la Administración, no implica que se realice según las previsiones de la normativa de protección de datos. Las cesiones a la Comisión de Escolarización, a la Universidad y a la Tesorería de la Seguridad Social tienen un amparo legal. Sin embargo, no todas las cesiones que se realizan a la Consejería de Educación están habilitadas legalmente, porque dependerá de la unidad solicitante de los datos personales y si existe alguna legislación que habilite la solicitud citada.

El resto de las cesiones que realizan los centros públicos, como la entrega del expediente académico completo al centro donde se traslada un alumno, la entrega de datos a

los Ayuntamientos, la entrega de datos a facultativos médicos externos o facilitar datos personales al AMPA, entre otros ejemplos, son cesiones que no cuentan con el consentimiento de los afectados ni de sus progenitores.

Se ha detectado que los centros concertados y privados realizan otras cesiones sin consentimiento. A modo de ejemplo se citan las siguientes: cuando los alumnos participan en certámenes y concursos se entregan datos de alumnos, y algunas veces de los padres, a la entidad organizadora del evento, a Asociaciones de Antiguos Alumnos, datos entregados entre alumnos a petición de uno de ellos y entrega de listados de clase a los padres de los alumnos que componen esa clase, incluyendo información relativa al nombre, apellidos y número de teléfono, domicilio e incluso si asisten a servicio de comedor y transporte. En algún caso, el orientador facilita a profesionales externos información sobre algún alumno fuera del ámbito de la prestación de servicios.

Se recomienda revisar todas las comunicaciones a terceros al objeto de detectar aquellas que no cuentan con habilitación legal y proceder a solicitar el consentimiento correspondiente.

PRESTACIONES DE SERVICIOS

En este apartado se analizó en qué momento acuden los centros escolares a terceras empresas para solicitarles la prestación de algún servicio y cómo está regulada la relación entre los centros escolares y la empresa seleccionada.

Los servicios más solicitados por los centros públicos son los gabinetes fotográficos que elaboran la orla, el servicio de transporte escolar, el de reparación y mantenimiento de los ordenadores, las actividades extraescolares o empresas que corrigen las pruebas psicopedagógicas. Muchos colegios también hacen de prestadores de servicios para el AMPA, sobre todo cuando se trata de realizar tareas de índole administrativa.

Cuando la Consejería de Educación contrata alguno o varios de los servicios citados anteriormente, los centros escolares desconocen el tipo de contrato que lo regula. Los servicios contratados directamente por los colegios nunca suelen estar plasmados en un contrato escrito y si el mismo existe, carece de las cláusulas correspondientes al artículo 12 de la LOPD. No obstante, la práctica habitual de los colegios es acudir a empresas para que les presten el servicio y abonar la factura correspondiente sin mediar ningún tipo de contrato.

Los colegios concertados acuden a asociaciones que les facilitan profesionales especializados para atender a niños con necesidades educativas especiales, empresas para gestionar el servicio de comedor, escuelas de música, agrupaciones deportivas, empresas donde realizan prácticas sus alumnos de formación profesional, servicios de tratamiento de datos, alojamiento de su página "web", empresas especializadas en maquetación de revistas y anuarios. Algunos colegios prestan sus servicios a la Asociación de Antiguos Alumnos o a la AMPA. La mayoría de las prestaciones de servicios se realizan

sin ningún contrato y, cuando existe el mismo, sin mención al artículo 12 de la LOPD. En algún caso sí se ha firmado un contrato adecuado pero puede considerarse como algo residual ya que no es la práctica habitual.

Los colegios privados también acuden a empresas externas que confeccionan y corrigen las pruebas psicológicas que realizan sus alumnos e incluso son los que elaboran los informes personalizados para cada alumno. Solicitan los servicios de psicólogos o médicos externos, empresas que retiran el papel para su reciclado, empresas de informática, servicios de comedor y transporte, actividades extraescolares, gabinetes fotográficos o empresas de seguros, entre otros. Estas prestaciones de servicios suelen realizarse, en una gran mayoría, sin un contrato alusivo al artículo 12 de la LOPD y se da el caso de alguna empresa que, prestando el mismo servicio en distintos colegios, con algunos ha firmado un contrato de prestación de servicios y en otros no consta un documento escrito.

En cualquiera de los casos, se recomienda que en los contratos de prestación de servicios en los que el contratista accede al tratamiento de datos por cuenta del responsable del fichero, el contrato se formalice por escrito y recoja los extremos a que se refiere el artículo 12 de la LOPD.

TRANSFERENCIAS INTERNACIONALES DE DATOS

Se pretendió conocer, en este punto, si los centros escolares remitían datos personales a entidades situadas fuera del territorio español y analizar, en su caso, si el procedimiento empleado se adecuaba a los dispuesto en la normativa de protección de datos. Ningún centro escolar público, entre los visitados, a excepción de dos institutos, realiza transferencias internacionales de datos. Las excepciones citadas son transferencias que se producen en el ámbito de intercambios internacionales para fomentar el aprendizaje de un idioma extranjero o para cursar la modalidad de bachillerato internacional. En los centros concertados y privados, tampoco se han detectado transferencias internacionales de datos, salvo en algún colegio privado, que se transfieren datos como consecuencia de intercambios de alumnos con el consentimiento de las familias.

En estos casos, si la comunicación de datos se efectúa a un país fuera de los que forman parte del Espacio Económico Europeo, salvo que exista una excepción legal, es preciso que el Director de la Agencia Española de Protección de Datos autorice dicha transferencia internacional de datos. Por el contrario, cuando no sea así, la comunicación puede realizarse teniendo presente la necesidad de formalizar la relación jurídica a través de un contrato que reúna las condiciones previstas en el artículo 12 de la LOPD.