

Memoria 2006

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



©AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
D.L: M-40187-2007
NIPO: 052-07-004-7

Diseño Gráfico: 

Imprime: NILO Industria Gráfica, S.A.





Por primera vez, desde mi nombramiento como Director de la Agencia Española de Protección de Datos tengo ocasión de presentar la Memoria de la entidad correspondiente al año 2006. Constituye, por tanto, un honor singular realizar esta presentación al referirse este documento a un periodo anterior al inicio en el ejercicio de mis funciones y, justo es reconocer que los indudables méritos y éxitos que en él quedan reflejados se deben, en lo que a su impulso se refiere, al notable esfuerzo y sobresaliente talento del anterior equipo directivo y del conjunto del personal al servicio de la Agencia.

La elaboración y publicación de la Memoria anual constituye una labor de especial importancia no solo por la relevancia de sus destinatarios iniciales -Ministerio de Justicia y Cortes Generales- sino también por suponer una forma de dar a conocer tanto a las instituciones públicas como privadas y, en general, a los ciudadanos la forma en la que se va materializando, en la práctica, la tutela del derecho fundamental a la protección de datos personales.

Esta Memoria presenta, como no podía ser de otro modo, una metodología semejante a la utilizada en los últimos años, buscando una cierta profundidad en la información proporcionada pero, al tiempo, intentando evitar ser prolijos en exceso a fin de facilitar su consulta y utilización por los operadores interesados.

En cualquier caso, quienes demanden una información más exhaustiva en materia de protección de datos de carácter personal, pueden acudir al fondo documental de la Agencia recogido en nuestra página web (www.agpd.es) donde se encuentran recopiladas normativa aplicable, resoluciones dictadas por la Agencia, informes jurídicos, consultas, sentencias dictadas en procesos en los que ha sido parte la Agencia y diverso material complementario.

De acuerdo con esta metodología, la memoria incluye un primer capítulo relativo al derecho fundamental a la protección de datos de carácter personal, que recoge una síntesis de los hitos más relevantes que han tenido lugar en 2006 y una referencia a las perspectivas de futuro haciendo hincapié en los distintos ámbitos en los que la Agencia pueda ofrecer un servicio de calidad al ciudadano. En dicho capítulo se subsume información que en el año 2005 figuraba bajo la rúbrica "Dirección" que, por ello se ha excluido de la presente Memoria. Asimismo el capítulo relativo a la naturaleza jurídica, régimen, estructura y funciones de la Agencia Española de Protección de Datos se ha trasladado al Anexo.

El segundo capítulo se centra en analizar pormenorizadamente las actividades realizadas por los diversos centros directivos integrados en la Agencia: correspondiendo los distintos epígrafes a la labor desarrollada por el Registro General de Protección de Datos, la Subdirección General de Inspección, la Secretaría General, el Área Internacional y el Gabinete Jurídico, siendo de destacar el notable incremento de actividad tanto desde un punto de vista cuantitativo como cualitativo.

Por otra parte, un tercer capítulo se dedica a los Códigos Tipo, cuya elaboración se sigue alentando desde la Dirección para mejor adaptar el cumplimiento de las exigencias de la Ley a las peculiaridades de los diferentes sectores.

Finalmente, la Memoria concluye con un apartado sobre la "Agencia en cifras" donde se proporciona información ordenada por medio de cuadros y estadísticas de gran utilidad para poder valorar de manera cuantitativa las distintas actividades desarrolladas por la Agencia en este ejercicio.

En definitiva, de los datos que se proporcionan en esta Memoria se deduce, como en años anteriores, el incesante incremento experimentado en la actividad de la Agencia y, a nuestro juicio resultara evidente para el lector, simplemente poniendo en relación la ingente actividad descrita en la Memoria, con los Recursos Humanos disponibles para llevarla a cabo, ya no solo la dedicación, sino incluso el esfuerzo del personal al servicio de la Agencia para intentar desarrollar satisfactoriamente las funciones que tiene encomendadas la Agencia Española de Protección de Datos Personales.

Sin embargo, aún queda mucho camino que recorrer y estamos dispuestos a ello trabajando por fomentar la existencia de una cultura de protección de datos personales en la sociedad, profundizando en las tareas de prevención como la realización de inspecciones sectoriales, el fomento de foros de debate, la suscripción de convenios de colaboración con otras entidades o instituciones cuya finalidad se orienta a la profundización en el conocimiento y ejercicio de este derecho, incrementando la cooperación con las Agencias Autonómicas de Protección de Datos, fomentando la autorregulación en las empresas o sectores de actividad, entre otras muchas áreas de actuación y sin olvidar nunca la evidente proyección internacional de este derecho.

Podemos concluir señalando que la sociedad española actual empieza a ser muy consciente de la importancia del derecho a la protección de datos personales en su vida cotidiana, así como de los peligros que los incesantes avances en la sociedad de la información dentro de un mundo globalizado pueden llegar a comportar sin una adecuada supervisión. En esta tarea de velar por el correcto cumplimiento de la legislación sobre protección de datos consideramos fundamental la labor desarrollada por la Agencia Española de Protección de Datos en los últimos años, una autoridad independiente y que ha cumplido con eficacia las labores de control encomendadas lo que le ha llevado a ser un referente internacional en la materia y esperamos, una vez recogido el testigo, seguir avanzando en esta línea de trabajo y, afrontando nuevos retos y proyectos, conseguir una mayor consolidación del derecho fundamental a la protección de datos de carácter personal.

ARTEMI RALLO

Director de la Agencia Española de Protección de Datos



INDICE

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: SITUACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO

- 17 UN DIÁLOGO PERMANENTE CON LA SOCIEDAD**
- 17 INCREMENTAR LA CONCIENCIACIÓN DE LOS CIUDADANOS
- 18 SIMPLIFICAR Y FACILITAR EL CUMPLIMIENTO DE LA LEY
- 20 MAYORES NIVELES DE SEGURIDAD JURÍDICA
- 22 UNA SOCIEDAD MÁS INFORMADA
- 22 LA DEFENSA DEL DERECHO**
- 23 LA PREVENCIÓN COMO ELEMENTO CLAVE
- 26 LA GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS Y LA IGUALDAD
- 27 LA ATENCIÓN SIN DILACIONES DE LAS RECLAMACIONES DE LOS CIUDADANOS
- 28 PROMOVER LA AUTORREGULACIÓN
- 28 OFRECER GARANTÍAS EN UN MUNDO GLOBALIZADO**
- 29 LAS TRANSFERENCIAS INTERNACIONALES DE DATOS
- 30 LA PROYECCIÓN INTERNACIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS
- 31 LA AEPD ANTE LOS NUEVOS RETOS INTERNACIONALES**

II ANÁLISIS DE ACTIVIDADES

- 37 REGISTRO GENERAL DE PROTECCIÓN DE DATOS**
- 37 INSCRIPCIÓN DE FICHEROS
- 44 RELACIONES CON LOS REGISTROS AUTONÓMICOS
- 44 PUBLICIDAD DE FICHEROS Y DERECHO DE CONSULTA
- 45 TRANSFERENCIAS INTERNACIONALES DE DATOS
- 49 SUBDIRECCIÓN GENERAL DE INSPECCIÓN**
- 49 ANÁLISIS ESTADÍSTICO
- 51 SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS. PROCEDIMIENTO DE ACTUACIÓN
- 53 RESOLUCIONES MÁS RELEVANTES
- 63 PLAN SECTORIAL DE OFICIO A LA ENSEÑANZA REGLADA NO UNIVERSITARIA
- 79 SECRETARÍA GENERAL**
- 79 NOTIFICACIÓN DE LAS RESOLUCIONES QUE DICTE EL DIRECTOR DE LA AGENCIA
- 80 EJERCICIO DE LA SECRETARÍA DEL CONSEJO CONSULTIVO
- 81 GESTIÓN DE LOS MEDIOS PERSONALES Y MATERIALES
- 84 GESTIÓN ECONÓMICO-ADMINISTRATIVA DEL PRESUPUESTO DE LA AGENCIA
- 85 EDICIÓN DE LOS REPERTORIOS OFICIALES DE INSCRIPCIÓN DE FICHEROS Y LA MEMORIA ANUAL DE LA AGENCIA
- 86 ORGANIZACIÓN DE CONFERENCIAS, SEMINARIOS Y CUALESQUIERA ACTIVIDADES DE COOPERACIÓN INTERNACIONAL INTERREGIONAL
- 86 PRESTACIÓN DEL SERVICIO DE ATENCIÓN AL CIUDADANO
- 88 LLEVANZA DEL INVENTARIO DE BIENES Y DERECHOS QUE INTEGRAN EL PATRIMONIO DE LA ENTIDAD
- 88 OTROS PROYECTOS DE INTERÉS PARA LA AGENCIA GESTIONADOS POR LA SECRETARÍA GENERAL

II ANÁLISIS DE ACTIVIDADES**91 AREA INTERNACIONAL**

91 TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES EN MATERIA DE PROTECCIÓN DE DATOS EN OTROS PAISES

EUROPA

92 ACTIVIDAD DERIVADA DE LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS: EL GRUPO DE TRABAJO DEL ARTICULO 29

98 PROPUESTAS LEGISLATIVAS RELEVANTES

IBEROAMERICA

105 LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

ESTADOS UNIDOS

107 COOPERACIÓN CON LA COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS

OTRAS ACTIVIDADES EN EL ÁMBITO INTERNACIONAL

107 CONFERENCIAS INTERNACIONALES DE PROTECCIÓN DE DATOS

109 I CONGRESO EUROPEO DE PROTECCIÓN DE DATOS

110 COOPERACIÓN EN LA LUCHA CONTRA EL SPAM: CONTACT NETWORK OF SPAM AUTHORITIES Y LONDON ACTION PLAN

110 CASE HANDLING WORKSHOP

111 GRUPO INTERNACIONAL DE TRABAJO DE PROTECCIÓN DE DATOS EN TELECOMUNICACIONES (IWGPDPT).

113 GABINETE JURÍDICO

113 INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

116 INFORMES SOBRE CONSULTAS PLANTEADAS POR RESPONSABLES DE FICHEROS

136 ANÁLISIS JURISPRUDENCIAL

151 INSTRUCCIÓN 1/2006

163 III. CÓDIGOS TIPO

INDICE

175 REGISTRO GENERAL DE PROTECCIÓN DE DATOS

- 176 EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD
- 176 FICHEROS INSCRITOS
- 176 INCREMENTO ANUAL
- 177 DATOS RELACIONADOS CON LA INSCRIPCIÓN EN 2006
- 176 OPERACIONES DE INSCRIPCIÓN
- 178 DATOS RELACIONADOS CON LA INSCRIPCIÓN DURANTE 2006
- 178 DISTRIBUCIÓN DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD
- 178 RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD
- 179 DOCUMENTOS DE ENTRADA SEGÚN EL TIPO DE SOPORTE DE LA NOTIFICACIÓN
- OPERACIONES DE INSCRIPCIÓN SEGÚN EL TIPO DE SOPORTE UTILIZADO PARA SU NOTIFICACIÓN Y EL TIPO DE OPERACIÓN REALIZADO
- 180 INSCRIPCIÓN DE TITULARIDAD PRIVADA
- 180 DISTRIBUCIÓN DE FICHEROS
- 182 DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS
- 182 DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES
- 183 DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD
- 184 DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS
- 184 FICHEROS CON CESIONES DE DATOS
- 185 DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD
- 186 INSCRIPCIÓN DE TITULARIDAD PÚBLICA
- 186 FICHEROS INSCRITOS: INCREMENTO ANUAL
- 186 DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN
- 187 DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL
- 187 DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS
- 188 DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL
- 190 DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS
- 190 DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS
- 191 DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES
- 192 DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD
- 193 DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS
- 193 FICHEROS CON CESIONES DE DATOS
- 194 TRANSFERENCIAS INTERNACIONALES DE DATOS
- 194 RESOLUCIONES DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES A TERCEROS PAÍSES CON NIVEL DE PROTECCIÓN NO ADECUADO
- 195 FICHEROS INSCRITOS QUE DECLARAN TRANSFERENCIAS INTERNACIONALES
- 196 DERECHO DE CONSULTA AL REGISTRO
- 196 DATOS SOBRE CONSULTAS AL APARTADO FICHEROS INSCRITOS EN LA WEB
- 197 ACCESOS AL CANAL DEL RESPONSABLE EN LA WEB

199 SUBDIRECCIÓN GENERAL DE INSPECCIÓN

- 200 ESTADÍSTICAS RELATIVAS AL REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN
- REGISTRO DE DOCUMENTACIÓN
- 201 ESTADÍSTICAS RELATIVAS A ACTUACIONES Y PROCEDIMIENTOS INICIADOS Y FINALIZADOS
- 201 ACTUACIONES Y PROCEDIMIENTOS INICIADOS (ÁREA DE INSPECCIÓN)
- 201 ACTUACIONES Y PROCEDIMIENTOS FINALIZADOS (ÁREA DE INSTRUCCIÓN)
- 202 ACTUACIONES PREVIAS DE INVESTIGACIÓN
- 202 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO
- 203 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL DENUNCIANTE
- 203 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL INVESTIGADO
- 204 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO
- 205 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR FINANCIERO
- XX205 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR DE TELECOMUNICACIONES
- 206 ACTUACIONES POSTERIORES A LA INSPECCIÓN
- 206 RESOLUCIONES DE ARCHIVO
- 207 PROCEDIMIENTOS SANCIONADORES INICIADOS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO
- 208 PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO
- 209 PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL IMPUTADO
- 210 PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR COMUNIDAD AUTÓNOMA EN LA QUE RADICA LA ADMINISTRACIÓN IMPUTADA
- PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR TIPO DE ADMINISTRACIÓN
- 211 PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS FINALIZADOS POR TIPO DE ADMINISTRACIÓN
- 212 TUTELAS DE DERECHOS
- 212 PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR DERECHO TUTELADO
- 212 PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR COMUNIDAD AUTÓNOMA DEL RECLAMANTE
- 213 RECURSOS DE REPOSICIÓN

215 SECRETARÍA GENERAL

216 RECURSOS HUMANOS

- 216 EFECTIVOS DE LA AGPD POR SEXO
- 216 RELACIÓN DE EFECTIVOS POR GRUPOS
- 217 RELACIÓN DE EFECTIVOS POR NIVELES

218 ÁREA DE ATENCIÓN AL CIUDADANO

- 218 CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO
- 218 COMPARACIÓN CON AÑOS ANTERIORES
- 219 EVOLUCIÓN DE LAS CONSULTAS PLANTEADAS A TRAVÉS DE INTERNET
- 219 ANÁLISIS DE LAS CONSULTAS POR TEMAS 2006
- 220 EXAMEN DEL APARTADO SOBRE DERECHOS 2006
- 221 ACCESOS A LA PÁGINA WEB AÑO 2006
- 221 EVOLUCIÓN GRÁFICA DE LOS ACCESOS WEB DURANTE EL AÑO 2006
- 222 COMPARATIVA ACCESOS WEB 2005-2006
- 223 REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006. COMPARATIVA CON AÑOS ANTERIORES
- 224 REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006 EN EL ÁREA DE ADMINISTRACIÓN GENERAL Y ATENCIÓN AL CIUDADANO. COMPARATIVA CON AÑOS ANTERIORES

225 GESTIÓN ECONÓMICA

- 225 PRESUPUESTO DE INGRESOS
- 225 ANÁLISIS CAPÍTULO MULTAS Y SANCIONES SOBRE DERECHOS RECONOCIDOS
- 226 PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULOS
- 227 PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULOS. OBLIGACIONES RECONOCIDAS
- 228 EJECUCIÓN PRESUPUESTARIA 2002
- 228 EJECUCIÓN PRESUPUESTARIA 2003
- 229 EJECUCIÓN PRESUPUESTARIA 2004
- 229 EJECUCIÓN PRESUPUESTARIA 2005
- 230 EJECUCIÓN PRESUPUESTARIA 2006
- 231 COMPOSICIÓN DEL INMOVILIZADO A 31 DICIEMBRE 2006
- 231 DETALLE DEL INMOVILIZADO A 31 DICIEMBRE 2006

233 AREA INTERNACIONAL

- 235 ASISTENCIA A REUNIONES EN EL ÁMBITO INTERNACIONAL DURANTE EL AÑO 2006

237 GABINETE JURÍDICO

238 INFORMES PRECEPTIVOS

- 238 EVOLUCIÓN DE INFORMES Y DISPOSICIONES
- 239 EVOLUCIÓN DE INFORMES PRECEPTIVOS

240 CONSULTAS PLANTEADAS

- 240 EVOLUCIÓN DE CONSULTAS 2002-2006
- 240 DISTRIBUCIÓN DE CONSULTAS 2006
- 241 DISTRIBUCIÓN DE CONSULTAS SECTOR PÚBLICO- SECTOR PRIVADO

242 CONSULTAS PLANTEADAS: DISTRIBUCIÓN SECTORIAL

- 242 DISTRIBUCIÓN DE LAS CONSULTAS POR SECTORES
- 243 EVOLUCIÓN CONSULTAS POR SECTORES (2005-2006)

244 CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

- 244 CONSULTAS POR MATERIAS
- 245 EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS (2005-2006)
- 246 CONSULTAS SOBRE CESIONES DE DATOS
- 247 CONSULTAS POR COMUNIDADES AUTÓNOMAS

248 CONSULTAS POR PROVINCIAS

249 SENTENCIAS: ÓRGANOS ENJUICIADORES

- 249 SENTENCIAS POR ÓRGANO JURISDICCIONAL

250 SENTENCIAS: SENTIDO DEL FALLO

- 250 SENTENCIAS DE LA AUDIENCIA NACIONAL
- 250 COMPARATIVA SENTENCIAS EN PRIMERA O ÚNICA INSTANCIA (PORCENTAJES)

251 SENTENCIAS: DISTRIBUCIÓN SECTORIAL

- 251 SENTENCIAS POR SECTORES
- 251 COMPARATIVA POR SECTORES

252 SENTENCIAS: DISTRIBUCIÓN POR MATERIAS

- 252 SENTENCIAS POR MATERIAS
- 253 COMPARATIVA DE SENTENCIAS POR MATERIAS (2003-2006)
- 254 SENTENCIAS SOBRE FICHEROS DE SOLVENCIA PATRIMONIAL
- 254 RESOLUCIONES EN CASACIÓN

Memoria

2006

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



ÍNDICE

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: SITUACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO

17 UN DIÁLOGO PERMANENTE CON LA SOCIEDAD

- 17 INCREMENTAR LA CONCIENCIACIÓN DE LOS CIUDADANOS.
- 18 SIMPLIFICAR Y FACILITAR EL CUMPLIMIENTO DE LA LEY
- 20 MAYORES NIVELES DE SEGURIDAD JURÍDICA.
- 22 UNA SOCIEDAD MÁS INFORMADA.

22 LA DEFENSA DEL DERECHO

- 23 LA PREVENCIÓN COMO ELEMENTO CLAVE
- 26 LA GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS Y LA IGUALDAD.
- 27 LA ATENCIÓN SIN DILACIONES DE LAS RECLAMACIONES DE LOS CIUDADANOS.
- 28 PROMOVER LA AUTORREGULACIÓN.

28 OFRECER GARANTÍAS EN UN MUNDO GLOBALIZADO

- 29 LAS TRANSFERENCIAS INTERNACIONALES DE DATOS.
- 30 LA PROYECCIÓN INTERNACIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS.

31 LA AEPD ANTE LOS NUEVOS RETOS INTERNACIONALES

I. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: SITUACIÓN ACTUAL Y PERSPECTIVAS DE FUTURO

UN DIÁLOGO PERMANENTE CON LA SOCIEDAD

Las Memorias de los últimos años y, en particular, la de 2005, han insistido en la necesidad de extender y consolidar en la sociedad la cultura de protección de los datos personales como un objetivo estratégico que puede alcanzarse en el medio plazo.

La consecución de este objetivo implica necesariamente un diálogo constante con la sociedad en el que pueden distinguirse dos colectivos específicos: los ciudadanos y los responsables del tratamiento de datos, tanto públicos como privados, como sujetos obligados a actuar conforme al sistema de garantías que establece la normativa de protección de datos personales.

Este diálogo comprende un abanico de objetivos entre los que necesariamente se incluyen los de promover un mayor conocimiento de sus derechos por parte de los ciudadanos, incrementar la seguridad jurídica para los sujetos obligados, simplificar y facilitar el cumplimiento de la normativa de protección de datos y alcanzar una sociedad más informada.

Los datos correspondientes al año 2006 ponen de manifiesto los avances alcanzados.

INCREMENTAR LA CONCIENCIACIÓN DE LOS CIUDADANOS

La oferta de información a los ciudadanos sobre el sistema de garantías del que son titulares se articula, básicamente, a través del Servicio de Atención al Ciudadano, el acceso a la página web de la AEPD, y la consulta al Registro General de Protección de Datos como instrumento diseñado por el legislador para permitirles conocer quiénes pueden ser responsables del tratamiento de sus datos personales y ejercer, a partir de esta información, los derechos que la Ley les reconoce.

En el año 2006 se han producido avances significativos en este ámbito, especialmente, a través de la oferta de los desarrollos tecnológicos que la AEPD ha ido poniendo a disposición de los ciudadanos.

En efecto, a lo largo del año la atención personalizada a los ciudadanos telefónica, presencial y por escrito, se ha mantenido estable, alcanzando la cifra de 35.839 consultas. Por el contrario, los accesos a la página web han tenido un importante incremento de casi el 45% (690.950 accesos adicionales), confirmando la importancia de este canal en la difusión de la normativa de protección de datos.

Asimismo el análisis de los accesos al RGPD ofrece un resultado satisfactorio en tal sentido, al constatarse que el derecho de consulta a través de la web se ha ejercitado en 1.056.650 ocasiones, en una proporción aproximada de dos a uno entre ficheros de titularidad privada y pública, respectivamente.

SIMPLIFICAR Y FACILITAR EL CUMPLIMIENTO DE LA LEY

Para facilitar el cumplimiento de la normativa de protección de datos es preciso mantener una actitud de constante diálogo con los sectores afectados con el fin de conocer sus dudas sobre tratamientos de datos complejos y analizar qué soluciones resultan adecuadas para resolverlas.

Este diálogo se articula, fundamentalmente, a través de la emisión de informes que den respuesta a las consultas planteadas por los responsables del tratamiento y de reuniones bilaterales dirigidas a anticipar los criterios que posibiliten un desarrollo lícito de sus actividades.

Los informes emitidos sobre consultas planteadas ante la Agencia ascendieron a 553, con un incremento de la complejidad de las cuestiones planteadas, descendiendo el volumen de consultas sobre cuestiones más sencillas o reiteradas en años anteriores. Estas consultas se reparten casi al 50% entre responsables públicos y privados.

En el año 2006, las reuniones mantenidas con responsables de ficheros sectoriales se han referido, en su mayor parte, a aquellos en los que se ha planteado un mayor número de reclamaciones. Entre ellos destacan las empresas y asociaciones del sector de las telecomunicaciones y servicios de la sociedad de la información; el sector financiero, donde merece una mención específica el desarrollo de nuevos servicios que faciliten a los ciudadanos la protección frente al fraude; el sector asegurador y el de publicidad y marketing directo.

Las citadas reuniones de trabajo se han ampliado, asimismo, a otros sectores como el de la automoción, o a los nuevos servicios que se están desarrollando en el aseguramiento sanitario privado vinculados a la historia clínica electrónica.

Entre los temas abordados resalta el relacionado con las nuevas modalidades en que puede ampararse la realización con garantías de transferencias internacionales de datos, como son las denominadas cláusulas corporativas vinculantes.

No obstante, la actividad de asesoramiento no ha quedado limitada a responsables del sector privado extendiéndose, también, a las Administraciones responsables de ficheros de titularidad pública con competencias, entre otros, en el ámbito de la salud, la actividad mercantil y financiera, los registros públicos, la administración electrónica o la seguridad.

En cuanto a colectivos de profesionales se han intensificado las relaciones con los gestores administrativos que, por su estrecha vinculación a las pequeñas y medianas empresas, constituyen un cauce apropiado para promover el conocimiento de la normativa de protección de datos entre las mismas.

Finalmente, adquieren particular relevancia las reuniones mantenidas con representantes de organizaciones sindicales, o con asociaciones orientadas a la defensa de los derechos fundamentales que constituyen un contrapunto necesario respecto de las perspectivas basadas estrictamente en legítimos intereses empresariales.

Las actividades descritas pretenden facilitar, como se ha señalado, el cumplimiento de la normativa de protección de datos.

En este sentido uno de los indicadores que tradicionalmente se han considerado relevantes para conocer el nivel de conocimiento de aquella normativa ha sido la evolución de las inscripciones en el RGPD.

En el año 2006 destaca que se hayan practicado en torno a 234.000 operaciones de inscripción, con un incremento neto de ficheros inscritos cercano a los 165.000 y una media de casi 1.000 operaciones diarias en el Registro (21% de incremento, que unido al acumulado de años anteriores permite constatar que en los últimos cuatro años se ha triplicado la actividad del Registro). Todo ello manteniendo un nivel satisfactorio en cuanto al cumplimiento de los plazos legales para la tramitación de los expedientes de inscripción.

Sin embargo, un análisis más detallado de estas cifras permite obtener algunas conclusiones significativas.

Así, el análisis de los sectores privados en que se ha producido crecimientos relevantes de ficheros inscritos indica que entre ellos se encuentran los relacionados con la educación, el turismo y la hostelería, lo que permite concluir que las inspecciones de oficio realizadas en estos sectores cumplen adecuadamente el objetivo de prevención al que están dirigidas.

La eficacia de las actuaciones de prevención se ha manifestado, también, en el ámbito de los ficheros de las Administraciones públicas, donde los requerimientos individualizados a Corporaciones locales ha permitido completar la inscripción de ficheros de los Ayuntamientos con población superior a 2.800 habitantes.

Por su parte, en el seguimiento de las finalidades declaradas en los ficheros inscritos se ha constatado un importante incremento de ficheros relacionados con la videovigilancia, circunstancia que, unida al aumento de reclamaciones sobre esta materia planteadas ante la Subdirección General de Inspección, ha aconsejado la aprobación por parte del Director de la Agencia de la Instrucción 1/2006, de 8 de noviembre, sobre videovigilancia, facilitando la adecuación del tratamiento de imágenes con fines de seguridad a los principios de la normativa de protección de datos.

No obstante, en el año 2006 brilla con luz propia en la actividad del RGPD la puesta en marcha del Servicio de Notificación **NOTA**.

Sin perjuicio de la descripción detallada que se recoge en otros apartados de esta Memoria destacan en el Sistema **NOTA** los siguientes aspectos:

- Su apuesta por un modelo de notificación simplificado, acompañado de notificaciones tipo ya preculminadas.
- El constituir el primer servicio de Administración electrónica de la AEPD, permitiendo la notificación y seguimiento de los expedientes a través de internet, mediante el uso de firma electrónica.
- Su flexibilidad, haciendo posible que quienes hayan de realizar inscripciones masivas puedan adaptar el sistema a sus propias herramientas de adecuación a la LOPD.

El Sistema **NOTA** se ha desarrollado siguiendo la normativa y los principios de Administración Electrónica, ha supuesto la creación del Registro Telemático de la Agencia Española de Protección de Datos y la celebración de convenios y acuerdos con otros organismos como el Ministerio de Administraciones Públicas y la Real Casa de la Moneda-Fábrica Nacional de Moneda y Timbre con el fin de utilizar los servicios que en este campo ofrecen. Así, por ejemplo, es posible utilizar los certificados de firma electrónica de los prestadores de servicios de certificación mas comunes, incluidos en la plataforma de validación afirma, o recibir, si así se desea, la notificación de la inscripción del fichero en el RGPD de forma telemática en la Dirección Electrónica Única del Servicio de Notificaciones Telemáticas Seguras (MAP-Correos).

Estas características del Sistema **NOTA** se enmarcan en una firme política dirigida a facilitar los responsables de ficheros el cumplimiento de sus obligaciones.

La opción por esta política permite confiar en que en un futuro próximo pueda resolverse el aspecto más negativo de la situación del Registro que corresponde a la deficiente inscripción de ficheros de pequeñas y medianas empresas, así como de profesionales, pese al aumento que se ha producido en 2006.

MAYORES NIVELES DE SEGURIDAD JURÍDICA

Resultaría reiterativo insistir, bajo esta rúbrica, en la importancia que implica el desarrollo reglamentario de la LOPD. En las Memorias de ejercicios anteriores se ha detallado con minuciosidad la necesidad de aprobación de esta norma fundada en el objetivo básico de alcanzar niveles superiores de seguridad jurídica en la aplicación de la normativa de protección de datos personales.

Basta destacar, con satisfacción, que el Ministerio de Justicia ha continuado en dicho año los trabajos de elaboración del proyecto de Reglamento, el cual ha sido sometido a informe preceptivo de la AEPD; circunstancia que implica que formalmente se ha iniciado el procedimiento de tramitación de la citada norma.

El informe emitido, coincidiendo en sus líneas básicas con el contenido del proyecto, ha tratado de aportar sugerencias adicionales para su mejora, partiendo de la experiencia práctica desarrollada por la Agencia en la aplicación de la LOPD durante los años transcurridos desde su entrada en vigor.

Mención específica merece en este ámbito la emisión de informes preceptivos en relación a proyectos o anteproyectos de disposiciones que, con carácter general, afecten a la normativa de protección de datos.

El efecto transversal de esta última en los más variados sectores objeto de regulación pone de manifiesto la importancia de garantizar una sistemática adecuada en el conjunto de normas que afecten al tratamiento de datos personales, evitando asimetrías e impulsando, como objetivo básico, mayores niveles de seguridad jurídica.

En el año 2006 se han sometido al parecer de la Agencia 73 disposiciones para la emisión de los correspondientes informes preceptivos. Cuantitativamente ello supone mantener un nivel de actividad análogo al del año anterior. Ahora bien, desde una perspectiva cualitativa el ejercicio al que se refiere esta Memoria se ha caracterizado por la importancia de las materias sobre las que la han planteado iniciativas normativas.

Entre ellas destaca, en el ámbito de las telecomunicaciones y la persecución de actividades criminales, el anteproyecto de Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, dirigido a transponer la Directiva 2006/24/CE.

También debe reseñarse, por lo que implica para el fomento del desarrollo tecnológico en el entorno de la Administración pública y de impulso a la accesibilidad confiable por parte de los ciudadanos a la actividad administrativa, el Anteproyecto de Ley de Administración electrónica.

En cuanto al tratamiento de datos especialmente protegidos, como son los de salud y, en particular, los datos genéticos, el año 2006 ha sido especialmente fructífero. Como muestra cabe citar los anteproyectos de Ley de bases de datos policiales sobre identificadores obtenidos a partir del ADN y de investigación biomédica. Entre ambos se lleva a cabo una regulación específica y garantista del tratamiento de datos genéticos, tanto en su vertiente de instrumento identificativo de las personas, como en la de base o fundamento para el desarrollo de la medicina.

Tampoco puede olvidarse, en lo que afecta a la garantía de valores constitucionales en la actividad deportiva, el anteproyecto de Ley contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

UNA SOCIEDAD MÁS INFORMADA

La Memoria del año 2005 ya incluía un apartado específico sobre esta materia en el que se destacaba la importancia de impulsar una más ambiciosa política de comunicación en la AEPD, dirigida a conseguir una mayor proximidad con los medios de comunicación, posibilitando la difusión de temas de actualidad y se informaba de la creación de un departamento específico al efecto.

Los datos del año 2006 acreditan el acierto de esta apuesta. En el pasado año se emitieron desde el Gabinete de Prensa más de 100 notas de prensa y comunicados sobre distintas cuestiones relacionadas con la actividad de la AEPD, de las que se hicieron eco distintos medios de comunicación. Asimismo se atendieron más de 300 demandas de información y solicitudes de entrevistas de distintos medios de comunicación, tanto especializados como de información general, y se han contabilizado cerca de 600 impactos y apariciones en medios de comunicación.

Sin embargo, los resultados obtenidos, con ser importantes, no pueden obviar la necesidad de realizar nuevos esfuerzos en un futuro inmediato.

En tal sentido se ha constatado la necesidad de reforzar el departamento de comunicación en su vertiente de promover unas relaciones intensas con los medios de comunicación con el fin, tanto de ampliar la difusión pública de las materias relacionadas con la protección de datos personales, como de atender las crecientes demandas de información por parte de aquellos.

Pero, sobre todo, se ha puesto de manifiesto la necesidad de integrar esta política de comunicación en una dimensión más amplia que incluya nuevos avances en la información difundida a través de la página web de la Agencia, haciéndola más actual y exhaustiva, e incrementado su calidad y complementándola con la puesta en marcha de un departamento de documentación que haga de la información facilitada por la Agencia un punto de referencia ineludible para todos aquellos que estén interesados en la protección de los datos personales. Tareas éstas que deberán abordarse sin dilación en el año 2007.

LA DEFENSA DEL DERECHO

Impulsar el diálogo con la sociedad no excluye, sino que tiene como presupuesto un funcionamiento efectivo de las autoridades independientes que tienen encomendada la función específica -sin perjuicio del control jurisdiccional- de garantizar con eficacia y sin dilaciones el sistema de garantías propio del derecho fundamental a la protección de datos personales, tanto en su dimensión preventiva, como en la dirigida a restablecer el cumplimiento de la norma en caso de infracción.

El ejercicio de estas funciones implica desarrollar actuaciones de carácter preventivo que reduzcan el riesgo de comisión de infracciones, ejercer la potestad sancionadora y de tutela de derechos en caso de incumplimiento, garantizar la cooperación entre la AEPD y las Agencias autonómicas de protección de datos en todos los órdenes, disponer de los recursos humanos y materiales necesarios para actuar eficazmente y promover la autorregulación.

LA PREVENCIÓN COMO ELEMENTO CLAVE

Intensificar la prevención significa, en primer lugar, facilitar a los responsables del tratamiento de datos el desarrollo de su actividad conforme a las exigencias de la Ley.

Pero supone, sobre todo, un beneficio para los ciudadanos en la medida en que el anterior objetivo implicará la garantía efectiva de sus derechos.

El conocimiento sobre la aplicación de la normativa de protección de datos no debe derivarse, como ha sido frecuente, de la resolución de procedimientos sancionadores y de tutela de derechos que señalen, "a posteriori", el camino a seguir.

Es preciso que los responsables del tratamiento puedan conocer, antes de que pueda producirse una infracción, los parámetros para llevar a cabo lícitamente su actividad.

La AEPD ha desarrollado una intensa actividad preventiva basada, fundamentalmente, en la realización de inspecciones sectoriales de oficio a través de las cuales se han auditado diversos sectores de actividad en el tratamiento de datos personales, tanto privados como públicos.

En lo que afecta a la presente Memoria debe indicarse que, como ya se informaba en la correspondiente al año 2005, en el mismo concluyó el trabajo de campo del plan sectorial de oficio al sector de la enseñanza reglada no universitaria.

En el año 2006 se ha procedido al análisis de la abundante información obtenida y se han elaborado las conclusiones y recomendaciones del plan, si bien fueron presentadas públicamente en enero de 2007.

El plan es consecuencia del compromiso asumido por el Director de la AEPD en comparecencia ante la Comisión Constitucional del Congreso de los Diputados.

Durante su desarrollo se han inspeccionado 61 centros de enseñanza públicos y privados, tanto concertados como no concertados.

La muestra seleccionada se ha dirigido a tratar de identificar íntegramente las deficiencias existentes respecto de la normativa de protección de datos personales, sin pretender un análisis cuantitativo exhaustivo del número de centros en los que se reiteran las mismas deficiencias.

Para su realización se han inspeccionado los tratamientos de datos de los alumnos y sus familias que realizan las distintas áreas y servicios de los centros de enseñanza, examinando aspectos como los formularios que emplean en los procesos de matriculación y solicitud de plaza y la tipología de datos y documentos que se recaban, los datos contenidos en el expediente académico, el tratamiento de datos por parte de los servicios médicos y de orientación de los centros, o las medidas de seguridad en materia de protección de datos implantadas en los centros escolares.

Las principales deficiencias detectadas se refieren al incumplimiento generalizado del deber de información exigido a la hora de recabar datos, comprobándose que los padres de los alumnos no son informados del destino de los datos personales que facilitan, de los tratamientos que va a realizar el centro escolar o la Consejería correspondiente, la finalidad y los destinatarios de la información; la recopilación de datos innecesarios en los procesos de admisión de alumnos, de matriculación y de gestión del expediente académico; la carencia de una política de cancelación de los datos recogidos durante los procesos citados; una deficiente implantación de las medidas de seguridad exigibles con el fin de que los datos personales de sus alumnos sean adecuadamente custodiados y no puedan ser conocidos por terceros no autorizados y la utilización de datos especialmente protegidos sin consentimiento expreso. Asimismo se ha constatado que cerca del 50 % de los Centros no han notificado sus ficheros con datos de carácter personal al Registro General de Protección de Datos.

El detalle de las conclusiones y recomendaciones se recoge en el apartado de la Memoria correspondiente a la Subdirección General de Inspección.

La amplitud de los aspectos comprendidos en las conclusiones y recomendaciones de dicha inspección sectorial, así como el cúmulo de deficiencias detectadas exigirán realizar actuaciones complementarias dirigidas a regularizar los incumplimientos de la normativa de protección de datos en un sector tan sensible.

Por otra parte, la inspección sectorial de oficio en la enseñanza reglada no universitaria ha ratificado la necesidad, ya conocida, de incentivar el conocimiento del derecho fundamental a la protección de datos desde los primeros años de la vida, de modo que forme parte de la vida cotidiana de los ciudadanos desde sus orígenes.

En este sentido, la AEPD ha impulsado, a comienzos de 2007, coincidiendo con la celebración del primer Día Europeo de Protección de Datos el pasado 28 de enero, diversas acciones de comunicación encaminadas a dar publicidad a esta celebración y a impulsar el conocimiento entre los ciudadanos de sus derechos y responsabilidades en materia de protección de datos.

Así, en primer lugar cabe destacar que la Agencia Española de Protección de Datos, con el objetivo de sensibilizar a los centros de enseñanza sobre el necesario cumplimiento de la normativa de protección de datos presentó las conclusiones y recomendaciones derivadas del Plan Sectorial de Oficio a la enseñanza reglada no universitaria" a responsables de los centros de enseñanza y consejerías de educación, y a los principales medios de comunicación del país.

También, se elaboraron y distribuyeron a más 14.000 centros de enseñanza consejos dirigidos a los menores sobre la utilización de sus datos personales, con el objetivo de difundir entre ellos el conocimiento de cuáles son sus derechos en materia de protección de datos, y de que puedan familiarizarse con un derecho fundamental, que pese a ser menos conocido, está presente en todas las facetas de sus vidas diarias.

De otro lado, aunque las inspecciones sectoriales han acreditado su eficacia para impulsar el cumplimiento de la normativa de protección de datos, como manifiestan los datos antes expuestos sobre la inscripción de ficheros en el RGPD, se ha constatado que deben ser completados con actuaciones adicionales.

En particular, es un hecho conocido que la constante evolución del tratamiento de datos personales, como consecuencia del desarrollo tecnológico, las exigencias de la globalización y las crecientes demandas de seguridad frente a los actuales fenómenos delictivos, hacen necesario que la AEPD lleve a cabo políticas activas que permitan analizar en detalle y ofrecer criterios sobre cómo debe garantizarse el derecho fundamental a la protección de datos personales ante estos nuevos retos.

En este sentido, resulta conveniente reflexionar sobre la articulación de foros de debate en los que, con participación de expertos en las distintas materias y representación de los sectores afectados, se evalúen y definan preventivamente las líneas de actuación que han de presidir el adecuado desarrollo de estas actividades.

De este modo se complementarán con acciones específicas y flexibles las iniciativas ya desarrolladas por la AEPD a través de la celebración de Protocolos de Colaboración con diversas entidades e instituciones para articular soluciones adecuadas en el tratamiento sectorial de datos personales, promover la difusión de este derecho y desarrollar acciones de investigación de carácter preventivo.

En 2006 cabe destacar el Convenio entre la Universidad de Alcalá de Henares que se enmarca en la apuesta tradicional de la AEPD de incorporar a la actividad universitaria una formación especializada en la materia, abrir nuevos cauces de investigación y permitir la realización de prácticas de alumnos en la Agencia.

No obstante, el impulso de estas modalidades de cooperación con la AEPD exigirá que, a partir de 2007, se activen los grupos de trabajo previstos en el amplio abanico de Protocolos ya vigentes y se pongan en marcha nuevos foros de debate en los que analizar los retos que se plantean en la sociedad.

El conjunto de acciones preventivas que se han descrito no ha impedido que se haya mantenido un incremento de las reclamaciones de los ciudadanos ante la Agencia por presuntas infracciones de la normativa de protección de datos.

Esta circunstancia ha dado lugar a que en el año 2006 se hayan incrementado en un 11% las actuaciones previas de investigación iniciadas (1.282).

Por su parte, los procedimientos sancionadores iniciados a responsables de ficheros de titularidad privada se han reducido a 281 habiéndose incrementado hasta

103 los correspondientes a responsables de titularidad pública. Las resoluciones de archivo de las actuaciones se han mantenido estables (137), y los procedimientos de Tutela de derechos iniciados (632) han crecido un 9%.

En cuanto al análisis por sectores de actividades, siguen resaltando "Telecomunicaciones" y "Entidades Financieras" como principales sectores objeto de actuaciones de investigación e inspección.

La suma de ambos sectores supone más del 50% de las actuaciones previas de investigación y casi la mitad de los procedimientos sancionadores finalizados por sector de actividad del principal imputado. Dentro del sector financiero las actuaciones previas de investigación se focalizan principalmente en el cumplimiento o incumplimiento de obligaciones dinerarias que deriva en la inclusión del afectado en un fichero de solvencia patrimonial. El envío de correos electrónicos y fax sin consentimiento de carácter comercial se erige como otro de los sectores en que las actuaciones de inspección tienen mayor importancia numérica.

Finalmente las reclamaciones relacionadas con la videovigilancia surgen en 2006 como un área en el que se ha incrementado la realización de investigaciones.

LA GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS Y LA IGUALDAD

La STC 290/2000, de 30 de noviembre, hace especial hincapié en la tradicional doctrina del Tribunal Constitucional, acerca de la exigencia de garantizar a todos los ciudadanos en lo que respecta a los derechos fundamentales y, entre ellos, el derecho a la protección de datos, condiciones de igualdad en todo el territorio del Estado.

Esta exigencia constitucional supone para la AEPD y las Agencias autonómicas de Protección de Datos la necesidad de coordinar sus competencias en todas las áreas de su actividad.

A partir del año 2005 las relaciones de cooperación con las Agencias Autonómicas de Protección de Datos han ido alcanzando progresivamente un mayor grado de institucionalización. Ésta se produjo inicialmente en el ámbito de los Registros de Protección de Datos, ampliándose posteriormente a los responsables jurídicos y enmarcándose tanto unas como otras en una reunión de Directores de las Agencias que se ha ido celebrando rotatoriamente en las ciudades sede de sus respectivas Entidades.

Todo ello sin perjuicio de la actuación coordinada en la investigación de presuntas infracciones de la LOPD y de la habitual participación en foros de difusión de la normativa de prestación de datos personales.

Durante el año 2006 este proceso se ha consolidado celebrándose por invitación del Director de la Agencia de Protección de Datos de la Comunidad de Madrid una reunión en julio de 2006.

Sin embargo, la experiencia adquirida en los dos últimos años y la complejidad de las materias que deben abordarse coordinadamente por las citadas Entidades, unido al proceso de reforma de diversos Estatutos de Autonomía, aconsejan llevar a cabo una reflexión más profunda sobre las fórmulas de cooperación que permitan alcanzar nuevos niveles de relación institucional, adaptando los parámetros propios de las Conferencias Sectoriales.

Las nuevas fórmulas de cooperación han de suponer, adicionalmente, una responsabilidad compartida en la dirección de los distintos grupos de trabajo que deban constituirse, de acuerdo con criterios basados en las competencias de unas y otras autoridades y las necesidades de especialización en los distintos ámbitos de actividad.

LA ATENCIÓN SIN DILACIONES DE LAS RECLAMACIONES DE LOS CIUDADANOS

Para el cumplimiento de sus objetivos la Agencia Española de Protección de Datos contó con unos recursos económicos durante el año 2006 de 9.764.185 euros lo que supuso un incremento de aproximadamente el 24.4 % con respecto al ejercicio anterior. A pesar del fuerte incremento presupuestario se alcanzó un grado de ejecución del mismo del 96.75% , lo que si bien supuso un esfuerzo inversor importante para poder ejecutar el presupuesto adecuadamente, permitió cubrir parte de las necesidades y objetivos del ente .

En relación con los recursos humanos, en la actualidad, la relación de puestos de trabajo de la AEPD se compone de 113 efectivos de lo que 110 corresponden a personal funcionario y 3 a personal laboral.

Los proyectos que han de acometerse requieren un nuevo planteamiento en cuanto a la dotación presupuestaria de la Agencia por lo que se ha propuesto un crecimiento del presupuesto para el ejercicio 2008 de aproximadamente un 45% con respecto al ejercicio 2007. Este presupuesto debe ser capaz de facilitar los medios humanos y materiales para atender el retraso en la tramitación de los expedientes sancionadores, (algo más de 1000 expedientes), sin olvidar las quejas del Defensor del Pueblo por el retraso en la garantía del derecho fundamental. El nuevo presupuesto debe permitir también, ejecutar los proyectos del DNI electrónico, la oficina virtual de atención al ciudadano e implementar políticas de difusión del derecho fundamental.

Así mismo, se hace necesario un crecimiento de la Relación de Puestos de Trabajo que permita en los próximos años casi duplicar la plantilla actual especialmente en el ámbito de la Inspección en el que las nuevas competencias normativas y el incremento de denuncias de los ciudadanos ha supuesto un aumento de más del 200% de expedientes sancionadores en los últimos años. Además la nueva Relación de Puestos debe atender con eficacia y sin dilación las demandas de los ciudadanos que acuden a la Agencia Española, no solo a cumplir con sus obligaciones legales, sino también en defensa de su derecho fundamental a la Protección de datos.

PROMOVER LA AUTORREGULACIÓN

Los Códigos tipo son instrumentos de autorregulación que ofrecen una vertiente preventiva en la medida en que suponen una adaptación de las exigencias legales a las especificidades de una determinada empresa o sector de actividad.

Sin embargo, para que los Códigos tipo puedan cumplir la función que se ha expuesto es preciso que no se limiten a ser una mera reproducción de las previsiones legales, sino que incorporen elementos de valor añadido tanto en lo que se refiere a la articulación de soluciones apropiadas para el sector o al incremento de las garantías legalmente exigibles, como en lo que afecta a los mecanismos internos que garanticen su aplicación efectiva por parte de las entidades voluntariamente adheridas.

En el año 2006 destaca la prestación del "Código Tipo de protección de datos personales del fichero VERAZ-PERSUS", que tiene como objetivo prevenir conductas perjudiciales para los ciudadanos y para el mercado, permitiendo que las personas que lo deseen puedan voluntariamente solicitar su auto-inclusión en dicho fichero para prevenir eventuales estafas por suplantación de su personalidad.

El Código fue inscrito en el Registro General de Protección de Datos antes de finalizar el ejercicio.

OFRECER GARANTÍAS EN UN MUNDO GLOBALIZADO

La Directiva 95/46/CE tuvo su origen en la necesidad de establecer un régimen de garantías armonizado que, protegiendo la información personal de los ciudadanos europeos, no supusiera, por la diversidad de regulaciones distintas de los EEMM, un obstáculo al desarrollo del mercado único.

De este modo, la Directiva partía de la exigencia de proteger los datos personales, pero sin que esta protección implicara un obstáculo al desarrollo del comercio entre países.

Esta opción de política legislativa ha permitido, según acreditó el Primer Informe de la Comisión Europea, de 15 de mayo de 2003, sobre la transposición de la Directiva en los distintos EEMM, garantizar un alto nivel de protección para los ciudadanos europeos compatible con el desarrollo de la actividad económica en Europa, si bien apunta la necesidad de realizar actuaciones correctoras puntuales en aras de alcanzar una mejor armonización.

Como resultado de la Directiva cabe afirmar que los ciudadanos europeos disfrutaban de un régimen de garantías que constituye un referente en el mundo globalizado en que nos encontramos.

Ahora bien, la garantía de este estándar de protección ha tenido como consecuencia el establecimiento de un riguroso y estricto régimen de autorizaciones para permitir que los datos personales de los europeos sean transferidos a terceros países que no ofrezcan un nivel equivalente de garantías en el tratamiento de los datos personales.

Rigor que es comprensible si se tiene en cuenta que, una vez transferidos a dichos terceros países, la información personal de los ciudadanos europeos puede ser objeto de tratamiento en cualquier lugar del mundo sin las garantías que nos ofrece nuestro espacio jurídico común.

Esta exigencia debe hacerse compatible, no obstante, con las necesidades de una actividad económica globalizada.

De ahí que sea necesario incentivar políticas que permitan compatibilizar ambas exigencias.

Estas políticas presentan una doble dimensión: Por una parte, la fijación de condiciones que posibiliten los flujos internacionales de datos con garantías adecuadas que debe cumplir el importador de datos en los terceros países que carecen de ellas. Y, por otra, estimular que dichos países, y no sólo las entidades importadoras de datos personales europeos, se aproximen al sistema de garantías de que disfrutaban estos ciudadanos haciéndolo extensivo a los de sus países, permitiendo, si es su intención, obtener una Decisión como países de nivel adecuado de protección.

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Durante el año 2006 se han incrementado tanto las solicitudes de autorización de transferencia internacional (54), como el número de autorizaciones resueltas (31).

Sin embargo, en el análisis de los datos de 2006 debe primar una perspectiva cualitativa, por delante de la meramente cuantitativa a la que se acaba de hacer referencia.

En efecto, atendiendo a la modalidad, objeto y destino de las transferencias internacionales autorizadas destacan tres fenómenos interrelacionados.

Por una parte, que la principal modalidad de transferencia es la que se lleva a cabo entre un responsable ubicado en España, principalmente dedicado a servicios de telecomunicaciones y una empresa prestadora de servicios en un tercer país (encargado del tratamiento), al amparo de las cláusulas contractuales tipo previstas en la Decisión de la Comisión Europea 2002/16/CE, de 27 de diciembre de 2001.

Por otra, que el objeto de tales transferencias se concreta en la prestación de servicios de atención al cliente y de promoción telefónica de nuevos servicios de telecomunicaciones.

Y, finalmente, que un número muy relevante de las mismas tiene como destino empresas ubicadas en países iberoamericanos (Chile, Colombia, Perú, Paraguay y Uruguay).

El conjunto de estos factores pone de manifiesto que se están produciendo decisiones empresariales autónomas que llevan consigo un fenómeno de deslocalización de actividades empresariales, en estos sectores y países, respecto de las cuales la obtención de una autorización de transferencia internacional de datos es un elemento instrumental necesario desde el punto de vista legal.

En este sentido debe partirse de la premisa de que el marco legal de las transferencias internacionales citadas resulta condicionado por las Decisiones de la Comisión Europea que han de ser asumidas por las Autoridades de Protección de Datos de los Estados miembros, entre ellas la AEPD.

Pero resulta igualmente necesario que en la autorización de la transferencia y en su ejecución posterior se analice detenidamente la eficacia de las garantías que las acompañan de manera que pueda constatarse que los derechos de los ciudadanos cuyos datos se exportan sean efectivos.

De otro lado, las consecuencias económicas y sociales de estos fenómenos aconsejan incentivar que en los expedientes de autorización intervengan, al menos en trámite de audiencia pública, las organizaciones representativas de quienes puedan considerarse afectados.

LA PROYECCIÓN INTERNACIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS

En el segundo de los aspectos antes indicados, la AEPD ha desarrollado, según consta en las Memorias de años anteriores una intensa actividad en este ámbito en una doble dimensión: liderando proyectos dirigidos a países hoy incorporados a la Unión Europea para colaborar en su adecuación al acervo comunitario e impulsando la actividad de la Red Iberoamericana de Protección de Datos

En esta área de actividad es una constante de las Memorias de la AEPD destacar el impulso a la Red Iberoamericana de Protección de Datos y la evolución de sus actividades para impulsar las iniciativas de los países iberoamericanos en el objetivo antes descrito.

Por ello merece una mención especial el impulso a las actividades de la Red Iberoamericana de Protección de Datos que sigue constituyendo una apuesta estratégica para el impulso del sistema de garantías sobre la protección de datos personales en los países iberoamericanos. En 2006 la Red ha elaborado documentos específicos sobre "Impulso Normativo y Armonización", "Instrumentos de Autorregulación" y "Tratamientos de Datos de Salud".

Como consecuencia de las actividades de la Red Iberoamericana, en el año 2006 se han puesto en marcha iniciativas por parte de algunos países del área con objeto de analizar

las garantías normativas e institucionales que les permitan obtener una decisión de adecuación por parte de la Comisión Europea.

No obstante, el impulso de naturaleza multilateral que suponen las actividades de la Red Iberoamericana no excluye, sino que se refuerza a través de iniciativas bilaterales que coadyuven al mismo objetivo.

En este sentido debe destacar la celebración en 2006 de diversas actuaciones convencionales.

Así, en el citado año 2006, se han firmado el Convenio Marco de Colaboración con la Universidad de Guadalupe (México), el Numeral 2 de la Carta de Intención para la colaboración en materia de protección de datos con el Instituto Federal de Acceso a la Información Pública de los Estados Unidos Mexicanos, así como con su homónimo del Estado de Puebla y el Convenio de Colaboración con la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP).

Las Carta de Intenciones y Convenios con las instituciones mexicanas descritas están orientados a intensificar, tanto en el plazo académico como en el estrictamente institucional, la difusión y consolidación de la cultura de protección de datos en países Iberoamericanos, reforzando las actividades multilaterales que realiza la Red Iberoamericana de Protección de Datos.

En esta misma línea, el importante Convenio suscrito con la FIIAPP contribuye de manera significativa a la consolidación de la citada Red Iberoamericana, aportando una infraestructura logística y organizativa imprescindible para la continuidad de sus actividades.

Este conjunto de actuaciones deberá complementarse en los años próximos con una intensificación de las acciones que permitan consolidar y ampliar una mayor participación institucional en la Red Iberoamericana de Protección de Datos que coadyuve a su estabilidad y constituya un presupuesto más sólido en el cumplimiento de sus objetivos.

Por otra parte, en 2006 se ha suscrito la Carta de Intenciones relativa a la Cooperación con la Agencia Andorrana de Protección de Datos que, además de promover en un marco institucional estable la cooperación y el intercambio de experiencias entre ambas Instituciones, abre un camino dirigido a promover las condiciones que permitan el reconocimiento del Principado de Andorra como país con un nivel adecuado de protección, facilitando los flujos internacionales de datos al mismo. A este respecto es preciso insistir en el avance que supondría la adhesión por parte del Principado de Andorra al Convenio 108 del Consejo de Europa.

LA AEPD ANTE LOS NUEVOS RETOS INTERNACIONALES

La protección de datos personales ha tenido siempre, como ponen de manifiesto las Memorias anuales de la Agencia, una fuerte proyección internacional.

En su origen esta proyección estuvo vinculada a los flujos internacionales de datos relacionados con el comercio mundial.

Posteriormente, el desarrollo tecnológico ha acentuado la dimensión internacional de la protección de datos en diversos aspectos entre los que merece una referencia especial la lucha contra el correo basura o "spam".

De otro lado, la exigencia de garantizar efectivamente el derecho de los ciudadanos ha planteado nuevos desafíos a las Autoridades de Protección de Datos en relación a cómo colaborar internacionalmente para hacer cumplir la Ley ("enforcement" en la terminología inglesa) y qué instrumentos son necesarios para ello. La mejora del "enforcement" pasa, así, a constituir una prioridad de las Autoridades de la UE.

Para estudiar estos últimos aspectos en el ámbito de la UE y formular propuestas, la AEPD ha liderado en los últimos años un grupo de trabajo (Enforcement Task Force), que ha centrado su estudio en una actuación de investigación sincronizada en un sector de la actividad económica, que se realiza por primera vez por todas las autoridades europeas de protección de datos, y cuyos resultados y conclusiones se aprobarán por el plenario del Grupo del Artículo 29 en 2007.

Sin embargo, en los últimos años, las cuestiones relacionadas con esta materia han adquirido un nuevo enfoque que afecta, prioritariamente, al tratamiento de datos con fines de investigación del terrorismo y otras formas graves de delincuencia organizada.

Como manifestaciones de esta tendencia cabe citar la transferencia de determinados datos de pasajeros (PNR) a las autoridades de los EEUU, el acceso por parte de estas últimas a datos sobre transferencias financieras (Swift), la Directiva 2006/24/CE relativa a la conservación de datos de tráfico y localización en servicios de telecomunicaciones, los intercambios de datos -entre ellos de ADN o huellas dactilares- derivados de la aplicación del Tratado de Prüm o, en términos más amplios, la reflexión sobre el sistema de garantías para la protección de los datos personales en el marco del III Pilar (Modificación de la base jurídica de Europol, establecimiento del Sistema de Información Schengen de 2ª generación - SIS II -, y la propuesta de Decisión Marco sobre protección de datos en materia de cooperación policial y judicial).

Esta situación ha obligado a una intensificación de las actividades internacionales de la AEPD, tanto en el Grupo del Artículo 29 de la Directiva, como en otros foros específicos entre los que destaca el Grupo de Trabajo de Policía que ha adquirido una particular relevancia ante esta nueva situación.

INDICE

37 REGISTRO GENERAL DE PROTECCIÓN DE DATOS

- 37 INSCRIPCIÓN DE FICHEROS
- 38 TITULARIDAD PRIVADA
- 39 TITULARIDAD PÚBLICA
- 42 SISTEMA **NOTA**

- 44 RELACIONES CON LOS REGISTROS AUTONÓMICOS
- 44 PUBLICIDAD DE FICHEROS Y DERECHO DE CONSULTA
- 45 TRANSFERENCIAS INTERNACIONALES DE DATOS

49 SUBDIRECCIÓN GENERAL DE INSPECCIÓN

- 49 ANÁLISIS ESTADÍSTICO
- 49 REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN
- 49 ACTUACIONES Y PROCEDIMIENTOS INICIADOS (ÁREA DE INSPECCIÓN)
- 50 ACTUACIONES Y PROCEDIMIENTOS FINALIZADOS (ÁREA DE INSTRUCCIÓN)

- 51 SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS. PROCEDIMIENTO DE ACTUACIÓN
- 51 UNIDAD DE INSPECCIÓN
- 52 UNIDAD DE INSTRUCCIÓN

- 53 RESOLUCIONES MÁS RELEVANTES
- 53 DATOS DE SALUD
- 55 INFORMACIÓN EN LA RECOGIDA DE DATOS (ARTÍCULO 5 LOPD)
- 56 CALIDAD DE DATOS (ARTÍCULO 4.3.LOPD)
- 56 CESIÓN DE DATOS (ARTÍCULO 11 LOPD)
- 58 CONSENTIMIENTO (ARTÍCULO 6 LOPD)
- 59 ADMINISTRACIONES PÚBLICAS
- 60 TUTELAS DE DERECHOS
- 61 COMUNICACIONES ELECTRÓNICAS COMERCIALES NO DESEADAS (ARTÍCULO 21 LSSI)
- 62 COMUNICACIONES COMERCIALES NO SOLICITADAS EN EL ÁMBITO DE LA LEY GENERAL DE TELECOMUNICACIONES

- 63 PLAN SECTORIAL DE OFICIO A LA ENSEÑANZA REGLADA NO UNIVERSITARIA
- 64 PRINCIPIOS DE INFORMACIÓN Y CONSENTIMIENTO
- 64 CENTROS PÚBLICOS
- 65 CENTROS PRIVADOS CONCERTADOS
- 65 CENTROS PRIVADOS NO CONCERTADOS
- 66 PRINCIPIO DE CALIDAD
- 66 CENTROS PÚBLICOS
- 67 CENTROS PRIVADOS CONCERTADOS
- 68 CENTROS PRIVADOS NO CONCERTADOS
- 68 DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS
- 69 INSCRIPCIÓN DE FICHEROS
- 69 DATOS ESPECIALMENTE PROTEGIDOS
- 69 CENTROS PÚBLICOS
- 70 CENTROS PRIVADOS CONCERTADOS
- 71 CENTROS PRIVADOS NO CONCERTADOS
- 71 MEDIDAS DE SEGURIDAD
- 71 CENTROS PÚBLICOS
- 72 CENTROS PRIVADOS CONCERTADOS
- 73 CENTROS PRIVADOS NO CONCERTADOS
- 74 DEBER DE SECRETO
- 75 CESIONES DE DATOS
- 76 PRESTACIONES DE SERVICIOS
- 77 TRANSFERENCIAS INTERNACIONALES DE DATOS

II. ANÁLISIS DE ACTIVIDADES

79 SECRETARIA GENERAL

- 79 NOTIFICACIÓN DE LAS RESOLUCIONES QUE DICTE EL DIRECTOR DE LA AGENCIA
- 80 EJERCICIO DE LA SECRETARÍA DEL CONSEJO CONSULTIVO
- 81 GESTIÓN DE LOS MEDIOS PERSONALES Y MATERIALES
- 81 GESTIÓN DE LOS RECURSOS HUMANOS
- 82 ACTIVIDAD DEL SERVICIO DE INFORMÁTICA
- 84 GESTIÓN ECONÓMICO-ADMINISTRATIVA DEL PRESUPUESTO DE LA AGENCIA
- 85 EDICIÓN DE LOS REPERTORIOS OFICIALES DE INSCRIPCIÓN DE FICHEROS Y LA MEMORIA ANUAL DE LA AGENCIA
- 86 ORGANIZACIÓN DE CONFERENCIAS, SEMINARIOS Y CUALESQUIERA ACTIVIDADES DE COOPERACIÓN INTERNACIONAL INTERREGIONAL
- 86 PRESTACIÓN DEL SERVICIO DE ATENCIÓN AL CIUDADANO
- 87 REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS 2006
- 88 LLEVANZA DEL INVENTARIO DE BIENES Y DERECHOS QUE INTEGRAN EL PATRIMONIO DE LA ENTIDAD
- 88 OTROS PROYECTOS DE INTERÉS PARA LA AGENCIA GESTIONADOS POR LA SECRETARÍA GENERAL

91 AREA INTERNACIONAL

- 91 TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES EN MATERIA DE PROTECCIÓN DE DATOS EN OTROS PAISES

EUROPA

- 92 ACTIVIDAD DERIVADA DE LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS: EL GRUPO DE TRABAJO DEL ARTICULO 29
- 98 PROPUESTAS LEGISLATIVAS RELEVANTES
- 98 PROPUESTA DE MODIFICACIÓN DEL PAQUETE DE DIRECTIVAS DE TELECOMUNICACIONES
- 99 EL TRATADO DE PRÜM
- 100 MODIFICACIÓN DE LA BASE JURÍDICA DE EUROPOL
- 102 ACTIVIDAD DERIVADA DE LOS CONVENIOS DE EUROPOL, SCHENGEN, SISTEMA DE INFORMACIÓN ADUANERO Y EUROJUST
- 102 OTRAS ACTIVIDADES EN EL MARCO EL TERCER PILAR
- 103 ACTIVIDAD DERIVADA DEL CONVENIO 108 DEL CONSEJO DE EUROPA
- 104 RELACIONES BILATERALES EN EL ÁMBITO EUROPEO

IBEROAMERICA

- 105 LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

ESTADOS UNIDOS

- 107 COOPERACIÓN CON LA COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS

OTRAS ACTIVIDADES EN EL ÁMBITO INTERNACIONAL

- 107 CONFERENCIAS INTERNACIONALES DE PROTECCIÓN DE DATOS
- 109 I CONGRESO EUROPEO DE PROTECCIÓN DE DATOS
- 110 COOPERACIÓN EN LA LUCHA CONTRA EL SPAM: CONTACT NETWORK OF SPAM AUTHORITIES Y LONDON ACTION PLAN
- 110 CASE HANDLING WORKSHOP
- 111 GRUPO INTERNACIONAL DE TRABAJO DE PROTECCIÓN DE DATOS EN TELECOMUNICACIONES (IWGPDPT).

113 GABINETE JURÍDICO

- 113 INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES
- 116 INFORMES SOBRE CONSULTAS PLANTEADAS POR RESPONSABLES DE FICHEROS
- 116 INTRODUCCIÓN
- 120 INFORMES DE MAYOR INTERÉS EMITIDOS DURANTE EL AÑO 2006
- 136 ANÁLISIS JURISPRUDENCIAL
- 136 INTRODUCCIÓN
- 137 SENTENCIAS DE MAYOR RELEVANCIA DICTADAS EN PRIMERA O ÚNICA INSTANCIA
- 145 SENTENCIAS DE MAYOR RELEVANCIA DEL TRIBUNAL SUPREMO
- 151 INSTRUCCIÓN 1/2006
- 151 ANÁLISIS GENERAL
- 153 LEGITIMACIÓN PARA EL TRATAMIENTO
- 159 CONSULTAS PLANTEADAS EN 2006 SOBRE ESTA MATERIA

II. ANÁLISIS DE ACTIVIDADES

REGISTRO GENERAL DE PROTECCIÓN DE DATOS

Las principales funciones del Registro General de Protección de Datos (RGPD) son aquellas relacionadas con la inscripción de ficheros de datos de carácter personal, de autorizaciones de transferencias internacionales de datos y de códigos tipo.

Asimismo, corresponde al RGPD velar por la publicidad de la existencia de los ficheros de datos de carácter personal. El art. 14 de la LOPD regula el derecho de consulta al RGPD, indicando que cualquier persona podrá recabar de forma pública y gratuita información sobre la existencia y finalidad de los ficheros y la identidad de su responsable, lo que le permitirá ejercer los derechos de acceso, rectificación, cancelación y oposición, que la Ley le reconoce.

También es de destacar, entre las actividades del Registro, las relaciones institucionales y de coordinación con los órganos correspondientes de las Agencias de Protección de Datos de Madrid, Cataluña y País Vasco al objeto de mantener actualizada la información registral.

El desarrollo de estas funciones por parte del RGPD durante el año 2006, ha estado acompañado de la puesta en marcha del nuevo modelo de notificaciones telemáticas a la Agencia, NOTA, en vigor desde el día 1 de septiembre.

INSCRIPCIÓN DE FICHEROS

En relación con la inscripción de ficheros, la actividad del RGPD ha continuado el progresivo crecimiento que se ha venido poniendo de manifiesto en años anteriores. Al finalizar 2006, se encontraban inscritos 815.093 ficheros, de los que 56.138 se corresponden con ficheros de titularidad pública y 758.955 pertenecen al sector privado, habiéndose producido un incremento neto de 164.360 ficheros respecto a 2005.

Durante el ejercicio 2006, se han practicado un total de 233.796 operaciones de inscripción, relativas al registro de nuevos ficheros, a la modificación y a la cancelación de inscripciones de ficheros, lo que supone que se han realizado, por término medio, 974 operaciones diarias. Esta cifra de operaciones supera en un 21% a la del año 2005, y teniendo en cuenta el crecimiento acumulado en los últimos años, se puede asegurar que en los cuatro últimos años se ha triplicado la actividad del Registro.

A pesar de este aumento de actividad en relación con las solicitudes de inscripción de ficheros, el RGPD ha podido mantener un nivel muy satisfactorio de respuesta en su tramitación, cumpliendo el plazo de un mes legalmente establecido en la LOPD. Para

precisar esta información, se puede señalar que el plazo medio de tramitación ha sido de 6 días naturales, plazo en el que fueron tramitadas el 70% de las solicitudes de inscripción. Así mismo, el 90 % de las notificaciones fueron tramitadas en 12 días naturales, pudiéndose destacar que el 20% de las solicitudes han sido tramitadas al día siguiente de la recepción de la solicitud en la AEPD.

Un elemento importante para mantener un nivel de respuesta adecuado en el proceso de inscripción de ficheros ha sido el sistema de notificaciones telemáticas a la Agencia (sistema NOTA) que, además de los elementos de simplificación y mejora que introduce en los nuevos modelos, incorpora novedades tecnológicas, como códigos ópticos de lectura que optimizan el uso de los recursos disponibles, de los tiempos de grabación de información, y por ende, de inscripción en el Registro.

Cabe señalar que durante el período inicial de implantación del sistema NOTA, los últimos cuatro meses del ejercicio, se realizaron un total de 5.866 operaciones de inscripción de ficheros que fueron notificadas mediante el formulario NOTA. Sin embargo, sólo en el mes de enero de 2007 ya se habían recibido 6.025 notificaciones mediante este sistema. Es de destacar que un 10% de las notificaciones recibidas mediante el sistema NOTA, se presenta a través del Registro Telemático de la Agencia, utilizando certificado de firma electrónica reconocido.

Aunque la puesta en marcha del sistema NOTA ha requerido ajustes técnicos y organizativos del RGPD, al cierre de esta memoria, se constata que aunque hasta el 1 de octubre de 2007 sigue siendo válida la presentación de solicitudes de inscripción de ficheros mediante el programa de ayuda que ha venido a sustituir NOTA, éste nuevo sistema ya se encuentra consolidado y está siendo utilizado de forma masiva.

TITULARIDAD PRIVADA

Los datos de inscripción de ficheros de titularidad privada del año 2006 revelan que es en el sector de la pequeña y mediana empresa, así como en el de profesionales en los que se han producido los principales incrementos de inscripciones. Sin embargo, dada la extensa proyección de estos colectivos, continúan siendo aquellos en los que todavía existe más deficiencia en cuanto al cumplimiento de la obligación de notificar los ficheros de datos personales al RGPD.

Los sectores de actividad que destacan principalmente en cuanto a mayores cifras de ficheros inscritos en 2006, son los relacionados con asesoría jurídica, auditoría, asesoría fiscal y el sector inmobiliario. Asimismo los sectores relacionados con la sanidad, la educación, turismo y hostelería se encuentran entre los que mantienen una importante actividad de notificación de ficheros al Registro.

Es importante observar la relación existente entre la inscripción de ficheros y las actividades desarrolladas por otras unidades de la Agencia, pues los datos señalados en el párrafo anterior ponen de manifiesto la repercusión de los planes sectoriales de oficio

que la Inspección ha desarrollado en el sector hotelero y en el de la enseñanza reglada no universitaria.

Los datos relativos a las finalidades declaradas en la notificación de ficheros pueden confirmar lo expresado anteriormente respecto a los sectores de actividad, ya que son la gestión de clientes, contable, fiscal y administrativa, la gestión de recursos humanos y nóminas, propias de los ficheros de una PYME o de un despacho profesional, las finalidades que presentan un mayor número de notificaciones. Por su parte, también deben destacarse las finalidades relacionadas con la prevención de riesgos laborales, la publicidad y prospección comercial, así como los servicios económicos-financieros y seguros.

Analizando la distribución geográfica de los ficheros inscritos, destaca Cataluña como la Comunidad Autónoma con un mayor número de ficheros seguida de la Comunidad de Madrid, Andalucía, Valencia, Galicia y Aragón. Esta distribución ha sido modificada respecto de años anteriores, y en 2006 es de destacar la iniciativa de responsables de Andalucía y Aragón, en relación con la inscripción de ficheros, que se ha visto incrementada en un 24 y en un 18 por ciento, respectivamente.

En cuanto a las notificaciones de ficheros recibidas en 2006 en las que se declara la recogida de datos especialmente protegidos, la práctica totalidad ha indicado el dato de salud (28.574) y/o afiliación sindical (8.892). Menos del 1% del total de ficheros inscritos en estas circunstancias declara datos de origen racial y/o vida sexual, y el 10% los de ideología, religión y/o creencias.

Los responsables que declaran el tratamiento de datos especialmente protegidos relativos a la salud de los afectados se enmarcan mayoritariamente en el sector de las actividades sanitarias (clínicas, oficinas de farmacia, etc) aunque también declaran este tipo de dato aquellos responsables que notifican tratamientos relativos a la gestión de la nómina de sus empleados y que incluyen el dato relativo al grado de minusvalía para el cálculo de la retención aplicable al Impuesto de las Personas Físicas.

Durante el año 2006 comenzaron a notificarse al RGPD una cantidad importante de ficheros relativos a videovigilancia, que en muchas ocasiones se acompañaban con el planteamiento de cuestiones relativas al cumplimiento de la LOPD en este tipo de tratamientos de datos. Estas cuestiones, entre otras, plantearon en la Agencia la necesidad de publicar una instrucción de videovigilancia. Al cierre de la memoria se ha apreciado el fuerte incremento de ficheros inscritos en el RGPD con estas finalidades.

TITULARIDAD PÚBLICA

El crecimiento del RGPD en relación con la inscripción correspondiente a ficheros de los que son responsables las Administraciones Públicas se mantiene en parámetros similares a los de años anteriores, situándose en torno al 14%.

En el análisis del crecimiento de ficheros inscritos distribuidos por el tipo de administración a la que pertenecen, se puede comprobar el efecto causado por las iniciativas del RGPD en relación con el proceso de información y requerimiento iniciado a finales de 2005 a los diferentes departamentos ministeriales que conforman la Administración General del Estado y a los Ayuntamientos de municipios con población superior a los 2.500 habitantes. Estas actividades se han reflejado en un aumento en el número de ficheros inscritos durante 2006 en ambos tipos de Administración.

En 2006 ha continuado la notificación de ficheros de titularidad pública de Colegios Profesionales y Cámaras de Comercio, Industria y/o Navegación, una vez asentados los criterios de delimitación de la titularidad de los ficheros de estas corporaciones, que se consolidaron en el año anterior.

Tal como se ha citado anteriormente, en relación con los ficheros de titularidad privada, en la inscripción de ficheros de las Administraciones Públicas también se constata que los ficheros que notifican datos especialmente protegidos, durante el año 2006, se refieren prácticamente en su totalidad a los datos de salud y de afiliación sindical. Y analizando las finalidades declaradas se puede comprobar que se trata de ficheros relacionados con recursos humanos y nómina. En este caso, también está relacionado con la notificación realizada durante 2006 de los ficheros correspondientes a los sistemas sanitarios de algunas Comunidades Autónomas y en especial la de Castilla y León.

Además, se ha incrementado el número de ficheros inscritos con datos relativos a la comisión de infracciones penales y/o administrativas, incremento que se corresponde con el aumento de los ficheros inscritos por los Ayuntamientos.

■ ADMINISTRACIÓN GENERAL DEL ESTADO

Como ya se ha citado anteriormente ha sido importante el número de operaciones que se han realizado en 2006 relacionadas con ficheros del ámbito de la Administración General del Estado, que ha alcanzado la cifra de 421 nuevas inscripciones.

Además de los departamentos ministeriales que tradicionalmente han destacado por mantener actualizada la inscripción de sus ficheros en el RGPD, como el Ministerio de Trabajo y Asuntos Sociales, y el Ministerio de la Presidencia, hay que señalar especialmente al Ministerio de Industria, Turismo y Comercio, que ha realizado una importante labor de actualización de la inscripción de sus ficheros, así como a los Ministerios de Fomento, Agricultura, Pesca y Alimentación.

■ ADMINISTRACIÓN AUTONÓMICA

En el ámbito de los ficheros correspondientes a las Administraciones Autonómicas es apreciable la mejora en la cantidad y calidad de la inscripción de ficheros de aquellas comunidades en las que existe una unidad administrativa con funciones de coordinación de la creación e inscripción de ficheros.

Sin perjuicio de la labor que desarrollan las Agencias Autonómicas de Protección de Datos en las Comunidades Autónomas de Madrid, Cataluña y País Vasco, de las que se informa en el apartado correspondiente, cabe destacar a la Consejería de Presidencia y Administración Territorial de Castilla y León, a la Oficina de Seguridad de la Información del Sacyl, la Dirección General para la Sociedad de la Información y las Telecomunicaciones de la Consejería de Industria y Tecnología de Castilla-La Mancha, la Dirección General de Calidad y Evaluación de las Políticas Públicas de la Xunta de Galicia, la Dirección General de Telecomunicaciones e Investigación de la Generalitat de Valencia y la Subdirección General de Inspección y Calidad de los Servicios de la Consejería de Economía y Hacienda de la Región de Murcia.

La Comunidad Autónoma de Andalucía ha sido la que más ficheros ha inscrito durante el año en estudio y la Comunidad Autónoma de Galicia también puede señalarse por haber continuado la inscripción de sus ficheros.

■ ADMINISTRACIÓN LOCAL

En cuanto a los ficheros inscritos por los entes locales, el aumento es bastante significativo, ya que en 2006 se tramitaron 3.857 inscripciones. En este aumento se encuentran los ficheros notificados por los Ayuntamientos de más de 2.500 habitantes que todavía no habían inscrito ningún fichero en el RGPD, y que habían sido requeridos al efecto en 2005. En relación con estos Ayuntamientos debe señalarse que en 2006 se dió traslado a la Inspección de Datos de la relación de entidades que no habían aportado ninguna documentación contestando al requerimiento, que inició los oportunos requerimientos de administraciones públicas. En el momento de cierre de esta memoria todavía se encuentran 50 de estos Ayuntamientos en trámites de notificación de ficheros.

En el estudio por provincias, el porcentaje mayor de ayuntamientos con ficheros inscritos en el RGPD corresponde a Huelva, con un 100% de ayuntamientos inscritos seguida de Almería, Pontevedra, Ciudad Real, Barcelona, Granada y Alicante.

Por lo que respecta al número de ficheros inscritos durante 2006 las provincias que han aumentado significativamente el número de ficheros inscritos de entidades locales son Ourense, Toledo, Zaragoza y Valencia.

Hay que señalar que el apoyo de instituciones como las Diputaciones Provinciales y los gobiernos autonómicos en el caso de las comunidades uniprovinciales resulta fundamental para que los pequeños municipios puedan conseguir el objetivo de tratar los datos personales de sus vecinos de acuerdo con lo previsto en la LOPD.

■ OTRAS PERSONAS JURÍDICO PÚBLICAS

En este apartado, además del incremento de inscripciones correspondiente a ficheros de titularidad pública de los Colegios Profesionales y de las Cámaras de Comercio, es

de destacar la actualización de la regulación de sus ficheros en relación con el art. 20 de la LOPD de la Asamblea Regional de Murcia, la Junta General del Principado de Asturias, y la propia Agencia Española de Protección de Datos.

SISTEMA **NOTA**

Mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006 (BOE nº 181, de 31 de julio), se aprobaron los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el RGPD (Sistema **NOTA**).

La entrada en vigor el día 1 de septiembre de 2006 de la citada Resolución ha puesto en marcha el nuevo sistema de notificación o sistema **NOTA**.

El sistema "**NOTA**", en vigor desde el 1 de septiembre de 2006, tiene por objetivo facilitar a los responsables de ficheros el cumplimiento de la LOPD, en particular la obligación de notificación de ficheros al RGPD. Para ello, el nuevo sistema se apoya en cuatro pilares básicos: la simplificación de la notificación a los responsables de ficheros, se convierte en el primer servicio de administración electrónica de la AEPD, incorpora funcionalidades que facilitan la comunicación con los registros autonómicos, y facilita al sector de la consultoría en materia de protección de datos la incorporación del sistema **NOTA** a sus herramientas de adecuación a la LOPD.

El nuevo sistema permite la notificación a través de Internet, mediante el posible uso de firma electrónica, en formato papel, incluyendo un código óptico de lectura para agilizar su inscripción; y en formato XML a través de Internet, con y sin certificado de firma reconocido.

El sistema **NOTA** está disponible en la página web, www.agpd.es, dónde cada responsable puede seleccionar el correspondiente formulario de inscripción de ficheros en función de la titularidad del fichero a notificar, pública o privada, utilizando una notificación simplificada o notificación tipo, ya precumplimentada que permite la notificación de ficheros tales como clientes, recursos humanos, nóminas, comunidades de propietarios, pacientes, o libro recetario de oficinas de farmacia de titularidad privada, o los ficheros de recursos humanos, gestión del padrón, gestión económica, o control de acceso de ficheros de titularidad pública, o bien mediante la notificación estándar, que permite la declaración de cualquier otro tipo de fichero.

En todo caso, el sistema **NOTA** incorpora una guía de ayuda para facilitar la cumplimentación de los formularios y orientar al responsable acerca de sus obligaciones sobre protección de datos.

Otras funcionalidades o mejoras del sistema **NOTA** son las relativas al seguimiento del estado de tramitación de las notificaciones remitidas a la AEPD a través de Internet, mediante el código de envío facilitado por el formulario electrónico.

Aunque la citada Resolución de 12 de julio de 2006 ha marcado la puesta en marcha del Sistema **NOTA**, también ha previsto un periodo transitorio de adaptación al nuevo modelo, estableciendo un período de convivencia entre los modelos aprobados mediante la Resolución de 30 de mayo de 2000 que, para el caso de las notificaciones presentadas en soporte papel, finalizó en diciembre del pasado año, y el próximo 1 de octubre de 2007 para el resto de soportes.

Desde septiembre de 2006 hasta la fecha de cierre de esta memoria, se puede afirmar que la opción de notificaciones precumplimentadas ha tenido una amplia aceptación por parte de los responsables de ficheros ya que una de cada tres notificaciones de alta notificadas con el formulario **NOTA** han optado por utilizar estas notificaciones tipo precumplimentadas.

Por otra parte, la Resolución de 12 de julio contemplaba la posibilidad de que tanto los responsables de ficheros como la industria, desarrollasen aplicativos que permitiesen el envío de notificaciones mediante programas propios siguiendo un sistema de intercambio basado en mensajes en formato XML, con o sin certificado de firma electrónica. Los formatos y especificaciones XML de titularidad pública y privada y el resto de información técnica necesaria pueden obtenerse libremente solicitándolos por correo electrónico, según se indica en el apartado correspondiente de la web de la Agencia.

Coincidiendo con que el día 1 de diciembre de 2006 finalizaba el plazo para la presentación de las notificaciones en formato papel, sistema ampliamente utilizado por algunos aplicativos suministrados a la pequeña y mediana empresa, y una vez que los suministradores de estos aplicativos han realizado las adaptaciones de los mismos al sistema basado en mensajes en formato XML, se ha observado un incremento sustancial en la utilización de este sistema durante los cuatro primeros meses de 2007, habiéndose tramitado en este periodo en el RGPD mas de 2.800 operaciones de inscripción correspondientes a notificaciones XML frente a las 4 notificaciones recibidas en el año 2006.

Tanto para las consultas e incidencias relacionadas con el formulario como el asesoramiento a los desarrolladores que deseaban utilizar el sistema de intercambio basado en mensajes en formato XML, la Agencia habilitó una dirección de correo electrónico con el fin de informar y resolver incidencias derivadas de la utilización del Sistema **NOTA** que ha completado la atención telefónica de la Agencia.

Por otra parte, la citada Resolución de 12 de julio de 2006 creaba también el Registro Telemático, habilitado para los procedimientos de notificación de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) con certificado de firma electrónica reconocido, así como para enviar notificaciones de ficheros a la AEPD mediante formato XML igualmente firmadas con certificado de firma electrónica reconocido.

RELACIONES CON LOS REGISTROS AUTONÓMICOS

Durante el año 2006 han continuado las reuniones y contactos con los representantes de las unidades de registro de ficheros de las Agencias Autonómicas.

En el encuentro de trabajo mantenido en el mes de julio en la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Española de Protección de Datos informó de los aspectos técnicos que ya habían sido acordados en reuniones anteriores, que habían sido incorporados en el desarrollo del nuevo sistema **NOTA**, que iba a entrar en vigor el 1 de septiembre de 2006. A este respecto, se ha facilitado toda la información y se han realizado las pruebas pertinentes con los diferentes Registros Autonómicos que desde ese momento, comenzaron los trabajos técnicos para adaptar sus envíos al Sistema **NOTA**, y que en algunos casos ya han concluido a primeros de 2007.

En el año 2006 y por el sistema anterior a **NOTA**, se han continuado recibiendo las notificaciones de ficheros de la Agencia de Protección de Datos de la Comunidad de Madrid, se han recibido y tramitado las primeras comunicaciones de la Agencia Vasca de Protección de Datos y se ha recibido la comunicación de la Agencia Catalana de Protección de Datos en la que se encontraban los ficheros tramitados por esta Agencia Autonómica en el año 2004.

PUBLICIDAD DE FICHEROS Y DERECHO DE CONSULTA

La publicidad del RGPD a efectos de facilitar el derecho de consulta regulado en el art. 14 de la LOPD se venía realizando a través de la página web de la Agencia en la que todos los meses se actualizaba el censo de ficheros inscritos en este órgano.

Como se mencionaba en la memoria de 2005, en el año 2006 se ha mejorado este servicio de consulta a través de la web para ampliar la información del contenido de la inscripción de cada uno de los ficheros y con una actualización diaria.

Como consecuencia de la publicación de la Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos, se procedió a adaptar la información que se hace pública en el catálogo de ficheros con datos de carácter personal inscritos en el RGPD disponible de forma gratuita en la página web de la Agencia, para facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 14 a 16 de la LOPD.

Según establece la citada Resolución, la información que se hace pública tanto en el catálogo disponible en la web de la Agencia, como el que se incorpora a la edición que

anualmente realiza la AEPD en formato CD-ROM, se corresponde con la información que el responsable del fichero ha notificado al Registro General de Protección de Datos en los apartados de responsable del fichero, servicio o unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación, identificación y finalidad y usos previstos del fichero, origen y procedencia de los datos, incluyendo el colectivo de personas sobre el que se obtienen los datos de carácter personal, tipos de datos, estructura y organización del fichero y, en su caso, los destinatarios de cesiones y/o transferencias internacionales de datos. Además, en el caso de los ficheros de titularidad pública, se publican los datos relativos a la disposición general de creación, modificación o supresión del fichero.

Es de destacar que mediante la publicación del catálogo de ficheros en la página web los ciudadanos han podido ejercitar el derecho de consulta a lo largo de 2006 en 1.056.650 ocasiones, 741.089 sobre ficheros de titularidad privada y 315.561 acerca de ficheros de titularidad pública.

Así mismo, desde el RGPD también se han atendido por escrito más de 2.300 consultas correspondientes tanto a ciudadanos que han utilizado este medio para consultar el registro, como por los responsables de ficheros que han solicitado copia del contenido de las inscripciones al objeto de regularizar las mismas.

TRANSFERENCIAS INTERNACIONALES DE DATOS

Se considera Transferencia Internacional de Datos a países terceros el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo. Este tratamiento puede suponer una cesión o comunicación de datos o bien tener por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

En relación con las comunicaciones de datos personales fuera del territorio español, se consideran países que proporcionan un nivel de protección adecuado los Estados que la Comisión Europea ha declarado, de conformidad con el artículo 25.2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, Suiza, Argentina, Guernsey, Isla de Man y Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

Asimismo, la Comisión ha declarado el carácter adecuado de las transferencias con destino a las entidades estadounidenses adheridas a los principios de "Puerto Seguro", así como el tratamiento y la transferencia de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos de América.

Los artículos 33 y 34 de la LOPD establecen el régimen al que habrán de someterse los movimientos internacionales de datos.

El artículo 33 establece que para realizar transferencias internacionales de datos a países que no proporcionan un nivel de protección equiparable al que presta la LOPD, será necesario solicitar una autorización para la transferencia que el Director de la Agencia solo podrá otorgar si se obtienen las garantías adecuadas.

La autorización de transferencia internacional de datos otorgada al amparo del artículo 33 de la LOPD requiere, al tratarse de un país que no ha sido declarado como país con un nivel de protección equiparable, la exigencia, a quien solicita la transferencia, de garantías adecuadas. Entre ellas se encuentran las concretadas en la Decisión de la Comisión 2001/497/CE de las Comunidades Europeas, de 15 de junio de 2001, relativa a las cláusulas tipo para la transferencia de datos personales a un tercer país de conformidad con la Directiva 95/46/CE, modificada por la Decisión de la Comisión 2004/915/CE de las Comunidades Europeas, de 27 de diciembre de 2004, y la Decisión de la Comisión 2002/16/CE de las Comunidades Europeas, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a los encargados del tratamiento establecidos en terceros países.

No obstante, el artículo 34 de la Ley, excepciona de la necesidad de autorización de transferencia a países que no proporcionan un nivel de protección adecuado, en los siguientes supuestos:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y

En los primeros meses de 2006 se ha resuelto la autorización de 15 expedientes iniciados a finales del año 2005, de los que 8 han tenido como país de destino los Estados Unidos de América, 1 Filipinas, 2 India, 1 China, 1 Hong Kong, 1 Malasia, y 1 Singapur.

Asimismo, el Director de la Agencia Española de Protección de Datos acordó el archivo de 5 solicitudes debido a que el solicitante no procedió a realizar las subsanaciones que le fueron requeridas para continuar con la tramitación del expediente de autorización.

Durante 2006 se han iniciado 54 expedientes de autorización de transferencia internacional de los que 31 han sido resueltos otorgando su autorización, de los que 8 han tenido como país de destino los Estados Unidos de América, 7 Chile, 4 Colombia, 4 Perú, 2 Filipinas, 1 India, 2 Marruecos, 1 Guatemala, 1 Paraguay y 1 Uruguay.

En este sentido, cabe señalar el aumento de solicitudes de autorización y el aún más significativo, más del doble, número de autorizaciones resueltas.

Respecto de estos expedientes iniciados durante el año 2006, el Director de la Agencia Española de Protección de Datos acordó el archivo de 10 solicitudes debido a que en 9 expedientes el solicitante no procedió a realizar las subsanaciones que le fueron requeridas para continuar con la tramitación del expediente de autorización y en 1 expediente el solicitante desistió de su petición.

Por último, al finalizar el año quedaron pendientes de resolver 13 expedientes con destino a Estados Unidos de América, Chile, Costa Rica, Marruecos, Méjico y Rumania. Al cierre de esta memoria, se puede adelantar que las transferencias han sido resueltas en los primeros meses de 2007.

Por lo que respecta al expediente de autorización a Rumania, el Director de la Agencia resolvió su archivo por la desaparición sobrevenida del objeto del procedimiento, debido a la incorporación de Rumania como miembro de la Unión Europea el día 1 de enero de 2007.

De los expedientes de autorización resueltos favorablemente durante el 2006, 43 transferencias internacionales fueron autorizadas cumpliéndose los requisitos de la Decisión de la Comisión 2002/16/CE de las Comunidades Europeas, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a los encargados del tratamiento.

En estos casos, las finalidades de las transferencias están en relación con la prestación de servicios de tratamientos relativos a la gestión y centralización de la facturación de los proveedores, clientes y gastos de los empleados, la prestación de servicios de tratamiento a efectos de integrar y optimizar la cadena de producción y suministro de componentes para la venta y distribución de productos de video doméstico, la prestación de servicios para la asistencia en relación con el desarrollo, mantenimiento y producción de los servicios bancarios básicos y del sistema de software de tarjetas de los clientes, la prestación de servicios de analítica comercial, la prestación de servicio para el soporte técnico de bases de datos, y la prestación de servicios consistentes en la atención telefónica de clientes y la prestación de servicios de acciones de marketing telefónico.

Es de destacar el crecimiento de autorizaciones en las que los exportadores de datos son entidades habilitadas para la prestación de servicios de comunicaciones electrónicas, entre ellas, telefonía, televisión y acceso a Internet; los importadores de datos están establecidos en países iberoamericanos y la finalidad es la prestación de servicios de atención y venta telefónica a sus clientes.

El resto de las transferencias internacionales (3) han sido autorizadas al verificarse que eran conformes a las garantías establecidas en el Conjunto I de la Decisión de la Comisión 2001/497/CE de las Comunidades Europeas, de 15 de junio de 2001, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a un tercer país previstas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

En estos casos, la finalidad de la transferencias internacionales fue la gestión centralizada en el área de recursos humanos.

La información relativa a las autorizaciones de transferencias internacionales de datos puede ampliarse consultando el texto de las correspondientes resoluciones, disponibles en la página web de la Agencia.

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.

De acuerdo con lo regulado en el RD 428/1993 por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, la Secretaria General asume principalmente las competencias propias de los Servicios Comunes y especialmente la gestión de los recursos humanos y la gestión económica del Organismo. Para explicar las actividades de la Secretaria General durante el ejercicio 2006 se seguirá el mismo orden establecido en el artículo 30 del mencionado Real Decreto.

- NOTIFICACIÓN DE LAS RESOLUCIONES QUE DICTE EL DIRECTOR DE LA AGENCIA.
- EJERCICIO DE LA SECRETARÍA DEL CONSEJO CONSULTIVO.
- GESTIÓN DE LOS MEDIOS PERSONALES Y MATERIALES
- GESTIÓN DE LOS RECURSOS HUMANOS.
 - ACTIVIDAD DEL SERVICIO DE INFORMÁTICA
 - GESTIÓN ECONÓMICO-ADMINISTRATIVA DEL PRESUPUESTO DE LA AGENCIA.
- EDICIÓN DE LOS REPERTORIOS OFICIALES DE INSCRIPCIÓN DE FICHEROS Y LA MEMORIA ANUAL DE LA AGENCIA.
- ORGANIZACIÓN DE CONFERENCIAS, SEMINARIOS Y CUALESQUIERA ACTIVIDADES DE COOPERACIÓN INTERNACIONAL E INTERREGIONAL.
- PRESTACIÓN DEL SERVICIO DE ATENCIÓN AL CIUDADANO.
- LLEVANZA DEL INVENTARIO DE BIENES Y DERECHOS QUE INTEGRAN EL PATRIMONIO DE LA AGENCIA.

Por último se incluirá un apartado referido a otros proyectos de interés que son gestionados por la Secretaria General que por su alcance o contenido se circunscriben dentro de las funciones propias de esta Subdirección General.

NOTIFICACIÓN DE LAS RESOLUCIONES QUE DICTE EL DIRECTOR DE LA AGENCIA

Durante el año 2006 se realizaron un total de 5.106 notificaciones. A lo largo del año 2006 se han remitido al BOE para su publicación un total de 74 resoluciones, ante la imposibilidad de practicar la notificación por el procedimiento ordinario. Es importante destacar la labor que realiza esta unidad ya que asume la responsabilidad de llevar

a buen término todo el procedimiento administrativo sancionador que culmina con la notificación no solo al denunciado sino también al denunciante y los otros interesados. Para una mejor gestión del procedimiento de las notificaciones se implantó en la Agencia el programa SICER que permite un seguimiento telemático en coordinación con el Servicio de Correos del estado de las notificaciones.

Para el desarrollo de las notificaciones la Agencia Española de Protección de Datos firma anualmente un contrato preferencial con la Entidad Correos para el procedimiento de notificación. Durante el año 2006 la Agencia pagó a la entidad Correos el importe de 156.006,43 euros por la realización de este servicio.

Otro aspecto importante a reseñar es el proceso de anonimización de las resoluciones sancionadoras y su traslado a la WEB de la Agencia Española de Protección de Datos en cumplimiento de la Instrucción 1/2004 de 22 de diciembre publicada en el BOE de 5 de Enero de 2005 de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones. En el ejercicio 2006 se han anonimizado un total de 1.327 resoluciones.

EJERCICIO DE LA SECRETARÍA DEL CONSEJO CONSULTIVO

A lo largo de 2006, el Consejo Consultivo se reunió en dos ocasiones, el 12 de julio y el 28 de diciembre.

En 2006 y con motivo del proceso de renovación de los miembros del Consejo Consultivo se publicó en el Boletín Oficial del Estado, la ORDEN JUS/3831/2006, de 15 de diciembre, por la que se dispone la publicación del Acuerdo del Consejo de Ministros por el que se nombran vocales del Consejo Consultivo de la Agencia Española de Protección de Datos (BOE 16 de diciembre de 2006) estableciéndose la nueva composición del Consejo Consultivo e incorporándose los siguientes miembros, por un lado D. Artemi Rallo Lombarte en representación de la Administración General del Estado y D. José Antonio Escudero López en representación de la Academia de la Historia en sustitución este último de D. Eloy Benito Ruano que dejó el cargo.

En el marco de la actividad del Consejo Consultivo, no sólo se debe destacar la labor realizada por éste en el apoyo a la gestión de la Agencia mediante la información puntual que el Director de la Agencia Española de Protección de Datos transmite a los miembros del Consejo Consultivo, sino que también es reseñable el papel de Consejo en la decisión del otorgamiento del Premio a la Protección de Datos y el Premio de Periodismo que fueron convocados por Resolución de 3 de marzo de 2006 publicados en el B.O.E. de 24 de marzo de 2006 y que el Consejo Consultivo en su sesión de Diciembre acordó dejar desierto ambos premios.

GESTIÓN DE LOS RECURSOS HUMANOS

La Relación de Puestos de Trabajo de la Agencia Española de Protección de Datos se compone de un total de 113 efectivos de los que 110 corresponden a personal funcionario y 3 a personal laboral. El número total de efectivos a 31 de diciembre sumaba un total de 98. El incremento en el número del personal destinado en la Agencia se produjo a través de la cobertura de puestos de trabajo mediante la resolución de los concursos de méritos publicados en el Boletín Oficial del Estado por Resolución de 25 de enero de 2006 (BOE 7 de febrero de 2006) y por Resolución de 10 de octubre de 2006 (BOE 24 de octubre de 2006) al terminar el ejercicio 2006 no se había resuelto este último concurso de personal convocado en el BOE que previsiblemente se resolverá en el primer trimestre de 2007. Estos concursos permitieron no sólo la incorporación de nuevo personal a este Ente sino también la promoción de funcionarios de la Agencia a puestos de superior nivel. En la parte de gráficos de la memoria se puede ver la distribución durante el año 2006 del personal por sexos, por grupos y por niveles.

Por lo que se refiere al Plan de Acción Social de la Agencia Española de Protección de Datos para la mejora de las condiciones socio-laborales del personal funcionario y laboral, se destinaron a esta finalidad 35.380 euros. El reparto de esta cantidad se realizó de la siguiente manera: al Programa de Apoyo al Transporte se destinaron 20.012,81 euros, al Programa de Ayudas Educativas para hijos 11.475,06 euros, al Programa de Estudios Oficiales 1.773,03 euros y al de Estudios no Oficiales 1.693,90 euros.

Por otra parte, se efectuó la tercera aportación al Plan de Pensiones de la Administración General del Estado al personal con destino en la Agencia, a fecha de 31 de diciembre de 2006, en función de grupo de pertenencia y de la antigüedad perfeccionada a esta fecha y cuyo importe total ascendió a 12.914,88 euros con un total de 97 partícipes.

En relación con la formación del personal de la Agencia, a lo largo de 2006 se culminó el proyecto iniciado el ejercicio anterior, en colaboración con el Instituto Nacional de la Administración Pública, para realizar un Plan de Formación Conjunto. En su virtud, en octubre de 2006, el Director de la Agencia aprobó el Plan de Formación interna 2006-2007 para los empleados del Organismo, compuesto por 11 actividades formativas, desarrollándose un curso de formación sobre la Ley 15/1999 de Protección de Datos Personales para los empleados de este Ente público, con una duración de 15 horas y con una participación de más de 30 funcionarios.

Otro aspecto importante es el referido al cumplimiento de la legislación vigente en materia de prevención de riesgos laborales en sus cuatro disciplinas preventivas, Seguridad en el Trabajo, Higiene Industrial, Ergonomía y Psicología Aplicada y Medicina del Trabajo. Para lo cual se llevaron a cabo las siguientes actividades, elaboración del Programa de Actividades, realización de la Memoria de Actividades

Preventivas, realización del Manual de Emergencia del edificio sede del centro de trabajo, detección de necesidades formativas, análisis ergonómicos de los puestos de trabajo y mejora de las pequeñas deficiencias detectadas y reconocimientos médicos voluntarios a 36 empleados.

Dentro de las relaciones sindicales con fecha 21 de diciembre de 2006 se creó en la Agencia la primera Sección Sindical en representación del sindicato UGT, con quienes se mantuvieron las reuniones adecuadas para coordinar la actividad del Organismo con la representación sindical.

ACTIVIDAD DEL SERVICIO DE INFORMÁTICA

El Servicio de Informática tiene encomendada la función de dar soporte en el manejo de las distintas herramientas de microinformática utilizadas, resolver las incidencias surgidas en la utilización de las aplicaciones específicas diseñadas para las distintas unidades de la Agencia, así como la instalación, mantenimiento y gestión de reparación de las instalaciones de hardware, comunicaciones y telefonía.

Este servicio se presta tanto a requerimiento de los usuarios como a iniciativa del propio Servicio de Informática, intentando mantener actualizadas las versiones de los distintos productos utilizados y mejorar algunos aspectos de desarrollo para un mejor manejo por parte de los usuarios.

En el proyecto NOTA, desde el Servicio de Informática se han realizado todas las labores relacionadas con la instalación y configuración de los servidores encargados de la recepción de estas notificaciones en un proveedor de servicios, así como el establecimiento de las distintas vías de comunicación que permiten que los usuarios puedan depositar estas notificaciones en el servidor, con o sin firma electrónica, validar la idoneidad de los certificados de firma, el registro telemático de las notificaciones, la descarga de las notificaciones a los sistemas locales de la Agencia para su tramitación y posteriormente la notificación de las resoluciones de inscripción por correo convencional o por vía telemática para aquellos usuarios que así lo hayan solicitado.

Para la realización de este proyecto, con la intención de extenderlo a otros proyectos dentro de la Agencia, se han suscrito diversos convenios de colaboración con algunas entidades, para la utilización de proyectos relacionados con la e-administración, tales como DNI electrónico y certificado CERES de la Fábrica Nacional de la Moneda y Timbre, para la utilización de sus certificados digitales en la firma electrónica y registro telemático de documentos; Plataforma de validación @firma del Ministerio para las Administraciones Públicas, a través del cual se realiza la comprobación de la idoneidad de los distintos certificados de firma recibidos, extendiendo el número de certificados válidos más allá del DNI y CERES a todos aquellos que se van incorporando a este proyecto y con el Servicio de Notificaciones Telemáticas Seguras del MAP y Correos, para la notificación telemática de las resoluciones de inscripción.

En la fase inicial de implementación de este proyecto fue necesaria la contratación de servicios de call center para la información a los usuarios y la resolución de las incidencias que pudieran surgir.

En relación con la aplicación SIGRID II, que sirve de herramienta de trabajo a la Inspección de Datos, la unidad de Informática ha realizado las labores de apoyo y coordinación del proyecto APLICACIÓN SIGRID II siendo el entorno tecnológico elegido para su desarrollo el lenguaje Java con J2EE, con servidor de aplicaciones OAS y gestor de base de datos ORACLE 10g, sobre plataforma Unix realizándose las labores de análisis y desarrollo correspondientes, así como de adquisición del hardware necesario, estando prevista la finalización de los trabajos de desarrollo e implementación a principios del segundo trimestre de 2007.

También durante el año 2006 se ha puesto en marcha un nuevo buscador en la página WEB que permite realizar búsquedas documentales en los más de 5000 documentos, de forma que a través de la selección de una, varias o todas las secciones existentes en la Web, se pueden buscar todas las palabras tecleadas, frases exactas, aquellos documentos que contengan alguna de las palabras o buscar por exclusión de las palabras tecleadas. Si se utilizan varios de estos criterios, el resultado final será la intersección de todos ellos.

Por otro lado y con el fin de disponer de un canal a través del cual poner a disposición del personal de la Agencia Española de Protección de Datos, de una forma rápida, ágil y cómoda, toda la información que pudiera ser de su interés en los temas relacionados con el desempeño de sus puestos de trabajo en la Agencia, se ha puesto en funcionamiento la INTRANET administrativa de la Agencia. En este portal, a través del navegador web, se han recogido funcionalidades como avisos, novedades y noticias; enlaces a las páginas web más accedidas, tales como la página web de la Agencia, BOE, Registro Mercantil e Industrial, base de datos de legislación Aranzadi, portal del empleo público Funciona; listín telefónico; resúmenes de prensa; sección de utilidades, en la que se aparecerán documentos de interés, formularios y modelos de uso común y software de uso común y libre distribución, formación, con actividades formativas de la Agencia y del INAP; Acción Social; tablón de anuncios y ofertas para el personal

También se ha desarrollado diversas utilidades como la aplicación para sincronizar agendas, el control de acceso al edificio y el movistar corporativo, que ha permitido un ahorro considerable del gasto telefónico, sin olvidar el apoyo técnico y coordinación de los trabajos para la instalación de proyectores, pantallas eléctricas, monitores de plasma, equipos de audio y video, videoconferencia, conexiones a ordenadores y a la red local para acceder a presentaciones locales y a aplicaciones de uso local o Internet, en el salón de Actos.

También es relevante el trabajo realizado para la tramitación de un convenio de suscripción al proyecto SICER de Correos y Telégrafos, que a través del intercambio vía correo electrónico de unos ficheros con un formato predeterminado, en el que se facilitan los datos identificativos de las notificaciones que se desean realizar, permite el tratamiento informático de esta información para su distribución y posterior comunicación del estado de recepción de las notificaciones.

El presupuesto inicial de la Agencia Española de Protección de datos para el ejercicio 2006 fue de 9.452.990 euros que se incrementó como consecuencia de las modificaciones presupuestarias hasta 9.776.418,58 euros. Este presupuesto ha supuesto un incremento del 21,81 % con respecto al presupuesto del ejercicio anterior. En 2006 lo más destacado ha sido la preparación del Presupuesto de la Agencia Española de Protección de Datos para el año 2007. El Presupuesto para el año 2007 es de 10.086.350 euros.

Por lo que respecta al estado de ejecución del Presupuesto de la Agencia se observa un porcentaje de realización global del 96,75 %, que no ha podido ser mayor debido a las vacantes producidas en la Relación de Puestos de Trabajo.

En relación con las modificaciones presupuestarias en el año 2006, de acuerdo con lo establecido en el artículo 34 del Estatuto de la Agencia que atribuye al Director la competencia para la realización de las modificaciones internas de presupuesto, se llevó a cabo una suplemento de crédito por importe de 317.775,58 euros destinado a sufragar gastos del Capítulo II y otro suplemento por importe de 5.653 euros para ajustar las dotaciones del complemento de productividad conforme a los establecido en las oportunas Ordenes Ministeriales de Economía y Hacienda. También se realizó una modificación presupuestaria con carácter de transferencia en la que se transfirieron 208.949,84 euros del capítulo I (artículo 12) al capítulo II (artículo 22).

Por lo que se refiere al gasto en capítulo 2 se centró principalmente en el pago del arrendamiento de la nueva sede institucional de la Agencia, así como los gastos corrientes generados por el pago de los servicios externalizados de seguridad y limpieza. También son importantes los gastos ocasionados por el Convenio con la Agencia Tributaria para el cobro por el procedimiento de apremio de las deudas generadas por el impago de las sanciones. Por último, la función inspectora de la Agencia, así como papel activo en el orden internacional de este Ente, genera un relevante gasto con cargo al capítulo II para el pago de dietas y locomoción.

La actividad de contratación, con cargo al capítulo 6 de la Agencia Española de Protección de Datos, durante el ejercicio 2006 se centró en tres grandes ámbitos. Por un lado, la adquisición de bienes necesarios para el desarrollo de la actividad ordinaria del Organismo, mediante la compra de mobiliario, fotocopiadores y material de oficina. Por otro lado, son importantes las inversiones en la adquisición de material informático, mediante la renovación y nueva adquisición de software y hardware y por último la contratación plurianual para la modificación del actual sistema de información de Registro General de Protección de Datos y de la aplicación SIGRIDII. También es interesante la contratación de una nueva Agencia de viajes por el procedimiento de concurso para la gestión de los viajes que en cumplimiento de sus funciones tienen que desarrollar lo empleados de la Agencia.

Asimismo es de destacar el análisis del Presupuesto de Ingresos de la Agencia porque, aunque asciende el porcentaje de ratio entre derechos reconocidos y las sanciones ingresadas, ya que, en términos globales, la recaudación creció por encima dos millones y medio de euros respecto del año anterior, ascendiendo a un total de 23.166.760,90 euros. Los derechos reconocidos durante el ejercicio ascendieron a 12.232.381,23 euros. Los datos pormenorizados aparecen recogidos en el apartado dedicado a la "Agencia en cifras".

Durante el año 2006 la Agencia se sometió a los habituales informes de control financiero por la intervención delegada, emitiéndose el informe definitivo con fecha 6 de septiembre de 2006. Con fecha 27 de septiembre de 2006 se publicaron en el BOE la aprobación definitiva de las cuentas anuales referidas al ejercicio 2006.

EDICIÓN DE LOS REPERTORIOS OFICIALES DE INSCRIPCIÓN DE FICHEROS Y LA MEMORIA ANUAL DE LA AGENCIA

Edición de los Repertorios Oficiales de Inscripción de Ficheros y la Memoria Anual de la Agencia

En el año 2006 se continuó la andadura ya iniciada en 1996, referida a la obligación estatutaria de editar, en soporte CD-Rom, el catálogo de ficheros del Registro General de Protección de Datos de la Agencia que contiene tanto las memorias anuales, la legislación vigente en protección de Datos tanto nacional como comunitaria, códigos tipo, publicaciones inscripción de ficheros, informes, resoluciones y otros textos de interés.

En ejecución del Plan Editorial para el año 2006, la Secretaria General de la Agencia Española de Protección de Datos, a través del Área de Administración General y Atención al Ciudadano, procedió a realizar las publicaciones que se detallan a continuación:

- PROTECCION DE DATOS DE CARÁCTER PERSONAL EN IBEROAMERICA.
2ª edición
- RED IBEROAMERICANA DE PROTECCION DE DATOS: DECLARACIONES Y DOCUMENTOS.
1ª edición
- PREMIO PROTECCIÓN DE DATOS PERSONALES. CONVOCATORIA 2005.
1ª edición
- MEMORIA 2005.
1ª edición.
- AGENCIA 2006.
1ª edición. CD ROM anual

Estas publicaciones se encuentran a disposición del público en general y no reportan pago o contraprestación alguna.

La Secretaría General asistió con voz pero sin voto a las reuniones convocadas por el Ministerio de Justicia para la aprobación del Plan Anual de Publicaciones del Ministerio de Justicia, que aprobó posteriormente el Consejo de Ministros.

ORGANIZACIÓN DE CONFERENCIAS, SEMINARIOS Y CUALESQUIERA ACTIVIDADES DE COOPERACIÓN INTERNACIONAL E INTERREGIONAL

Del 24 al 28 de julio de 2006, tuvo lugar en la el Real Sitio de San Lorenzo de El Escorial Santander un curso de verano bajo el título " El Reglamento de desarrollo de la Ley Orgánica de Protección de Datos", que fue un foro de encuentro importante en el que se debatió el borrador de proyecto de reglamento en desarrollo de la Ley Orgánica de Protección de Datos Personales.

Por otro lado la Secretaría General colaboró intensamente con la Unidad de Internacional para la organización de viajes en los que institucionalmente participó la Agencia, especialmente en la organización del Congreso Europeo de Protección de Datos y en el Encuentro con la Comisión de Protección de Datos de Portugal.

También es destacable la organización del DÍA DE PUERTAS ABIERTAS DE LA AGENCIA, para los hijos del personal de la Agencia en el que se trataba de difundir el Derecho Fundamental a los hijos de los empleados del Organismo.

Por otro lado en coordinación con la Subdirección General del Registro se realizó la presentación a los medios de comunicación y a las empresas del sector el programa NOTA que tuvo lugar en el Casino de Madrid el día 12 de julio de 2006.

PRESTACIÓN DEL SERVICIO DE ATENCIÓN AL CIUDADANO

Esta área constituye, en la mayoría de las ocasiones, la primera aproximación que tiene a su disposición el ciudadano para poder informarse y plantear aquellas consultas que considere necesarias en orden a la aplicación de la LOPD a su caso concreto. Ello implica, como ya se ha venido poniendo de relieve en memorias anteriores, que una de las funciones primordiales de este área es tratar de informar a los ciudadanos, de la forma más sencilla posible, sobre aquellas cuestiones que les preocupan directamente, facilitándoles la orientación y ayuda que precisen para una mejor defensa de sus derechos, e indicándoles los diferentes aspectos que se regulan en la LOPD y en el resto del ordenamiento jurídico de aplicación en esta materia.

En función de las diferentes formas en que se presta la atención al ciudadano, se pueden distinguir dentro de esta área, de una parte, la atención personalizada y de otra parte, la información que se obtiene directamente a través de la página web de la Agencia.

Por lo que se refiere a la atención personalizada, la misma se viene realizando, al igual que en cualquier otro órgano de la Administración pública, de tres formas distintas: la atención telefónica, la atención presencial y la atención por escrito. El número de consultas atendidas en el año 2006 ha representado un total de 35.839 consultas. Se puede señalar que la atención personalizada al ciudadano es ligeramente superior a la del año 2005, con un incremento de 327 consultas netas, lo que representa un aumento del 0,9 por ciento.

La contestación de consultas escritas se realiza también por Internet. Los meses de septiembre, octubre y noviembre de 2006 fueron los que canalizaron un mayor número de consultas a través de este medio, siendo noviembre el más activo con un 12% del total anual. En el año 2005, sin embargo, los meses con más actividad en las consultas web fueron febrero y marzo.

En lo relativo a la clasificación de las consultas por temas, se observa que los ciudadanos han seguido preocupándose fundamentalmente por conocer cómo deben ejercitar mejor sus derechos, en una tendencia que se mantiene pareja respecto al año 2005. Dentro de los derechos, los ciudadanos se han interesado mayoritariamente por informarse sobre cómo ejercitar el derecho de cancelación, siguiendo, igualmente, la tónica observada desde el año 2004.

En lo relativo a la información obtenida a través de la página web se observa que el mes en el que se realizó mayor número de accesos por parte de los ciudadanos/usuarios fue septiembre, seguido del mes de junio, modificándose la tendencia observada desde el año 2004 y continuada en el año 2005, en los que el mes de mayor actividad en este sentido fue el mes de octubre. Durante el año 2006 se produjeron un total de 1.538.714 accesos a la página web, frente al año 2005 que fue de un 847.764 lo que supone un incremento de 690.950, equivalente al 44,90 %.

Se destaca que la página web de la Agencia posee nivel de accesibilidad doble "a" para personas con discapacidad.

REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006

Se incluye nuevamente en una Memoria de este Organismo la estadística relativa al Registro de entrada y salida de documentos, actividad que absorbe casi el 50% de la desarrollada en este Área. El Registro de Entrada y Salida ejerce funciones generales de registro de toda la Agencia por lo que en términos globales se constatan los siguientes datos, que aparecen desglosados en la Memoria en cifras:

El número total de registros de entrada y salida de documentos efectuados en el Área de Atención al Ciudadano durante el año 2006 ha sido de 123.462, repartidos de la siguiente manera: 116.318 registros de entrada y 7.144 de salida, lo que supone un incremento de 25.183 registros más respecto del año 2005, es decir, un 25,62% más, en términos porcentuales.

El número total de registros de entrada y salida de toda la Agencia Española de Protección de Datos ascendió a 357.471 documentos de los que 124.362 corresponden a la entrada y 233.109 a la salida de documentos.

Estos números suponen que el 93,53% aproximadamente del registro de entrada de documentos en la Agencia se realiza en el Área de Administración General y Atención al Ciudadano. En el año 2005, este porcentaje era del 71 %.

De igual manera, este Área absorbe el 3,06 % del registro de salida de documentos que genera el Organismo. En el año 2005, este porcentaje fue del 37,44 %. Esta disminución se explica porque se permitió, durante el año 2006, registrar salidas a las distintas Unidades de la Agencia, dado que en Atención al Ciudadano no eran asumibles, por su elevado volumen

LLEVANZA DEL INVENTARIO DE BIENES Y DERECHOS QUE INTEGRAN EL PATRIMONIO DE LA ENTIDAD

Con motivo del cambio de sede institucional de la agencia se programó que durante el año 2006 se realizase una revisión exhaustiva del inventario de bienes y derecho de la Agencia Española de Protección de Datos. A 31 de diciembre el inventario se compone de un total de 2.989 bienes. A esa misma fecha se dieron de baja aquellos bienes deteriorados que estaban guardados en almacenes y en desuso, que ya no eran utilizables en la nueva sede como a la baja en inventario de material informático inservible. El valor neto del inmovilizado a 31 de diciembre de 2006 era de 2.002.580,59 €

OTROS PROYECTOS DE INTERÉS PARA LA AGENCIA GESTIONADOS POR LA SECRETARÍA GENERAL

Sin perjuicio de lo anterior la Secretaría General desarrolla otros cometidos que si bien no se encuentran enmarcados dentro de las competencias que recoge el Estatuto de la Agencia, si que son propios de las funciones de la Secretaría General del Ente Público. Así cabe destacar la organización de diversos cursos en el ámbito de los Planes de Formación de los diferentes Departamentos Ministeriales con la finalidad de contribuir a la formación de los empedados públicos en la materia de la Protección de Datos. Se destacan los cursos de formación impartidos en el INAP, Ministerio de Trabajo y Ministerio del Interior.

Especial mención merece los esfuerzos realizados para la tramitación de un Convenio de colaboración en la materia de formación sobre el Derecho Fundamental con el sindicato de CCOO que previsiblemente se firmará a lo largo del ejercicio 2007.

Otro proyecto de intereses es el relacionado con la la creación de una biblioteca especializada en materia de protección de datos. Para ello, el nuevo edificio dispone de un espacio de aproximadamente 500 m2 en los que ubicarla. Durante el año 2006 se han continuado los trabajos preparatorios de este proyecto y se ha realizado un análisis de inversiones, además se ha comenzado a recibir aportaciones bibliográficas de los diferentes Ministerio así como la adquisición de un fondo de libros.

En virtud de las atribuciones establecidas por el artículo 37. 1) de la Ley Orgánica 15/1999 de Protección de Datos, la Agencia Española de Protección de Datos tiene encomendada la labor de "...desempeñar las funciones de cooperación internacional en materia de protección de datos personales".

En el ejercicio de esa competencia, la AEPD lleva a cabo una intensa actividad internacional en distintos ámbitos geográficos participando en diversos foros de debate y consultivos, así como desarrollando actividades de supervisión y cooperación tanto multilateral como bilateralmente.

TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES EN MATERIA DE PROTECCIÓN DE DATOS EN OTROS PAÍSES

Además de analizar nuestra propia actividad y objetivos en el ámbito internacional, de acuerdo con lo previsto en el artículo 8.1.b del Estatuto de la AEPD, se describen en este apartado de la Memoria cuáles han sido las principales tendencias legislativas, jurisprudenciales y doctrinales en materia de protección de datos en otros países e instituciones.

La Comisión Europea ha seguido la tendencia iniciada en el año anterior de vigilancia de los acuerdos que podríamos llamar "transatlánticos" de transferencia de datos. Además, en este año 2006 ha iniciado la negociación, por mandato de los Estados Miembros, de un Convenio con las autoridades competentes norteamericanas que regulará la transferencia de datos de pasajeros de aerolíneas desde Europa a aquél país con una vocación de permanencia (frente al acuerdo temporal que existe actualmente con vigencia hasta julio de 2007). En esta misma línea de actividad, la Comisión Europea interviene, desde la aparición en julio de 2006 de un nuevo caso de transferencias transatlánticas no autorizadas en materia financiera, junto con las autoridades de protección de datos de los Estados Miembros, para poner fin a la posible situación de ilegalidad creada. La información pormenorizada sobre las actividades de la Comisión se puede consultar en el 10º Informe Anual del Grupo del Artículo 29.

En el entorno de los Estados Miembros de la Unión Europea se observa la creciente tendencia de las autoridades encargadas de la lucha contra delitos de terrorismo y formas graves de criminalidad a disponer en sus investigaciones del mayor número posible de información personal relacionada con el uso de las telecomunicaciones, posibilidad prevista en la Directiva Europea de Retención de Datos (D 2006/24/EC). La transposición a los ordenamientos internos de esta Directiva ha constituido durante este año una tarea esencial de los legisladores nacionales. Se observa igualmente una creciente actividad normativa en el ámbito de los documentos y sistemas

de identificación digital (ya sean a los efectos de simple identificación o para acceder a servicios sanitarios o de gobierno electrónico). Los diferentes desarrollos normativos en los distintos países se incluyen en el informe anual del Grupo de Autoridades Europeas de Protección de Datos correspondiente al año 2006 .

En el ámbito Iberoamericano se observa un desplazamiento desde el sector jurídico-público al económico para impulsar sus estándares de protección de datos a los de la Unión Europea, favoreciendo de esta forma el libre de flujo de información entre los actores económicos, requisito necesario para las transacciones comerciales en ambos continentes. En este proceso, la AEPD ha iniciado en 2006 los contactos con la Corporación para el Fomento de la Economía de Chile para prestar la asistencia técnica necesaria para alcanzar dichos objetivos y con el Instituto Federal de Acceso a la Información Pública de México. Los desarrollos normativos en materia de protección de datos producidos en los distintos países de la región pueden consultarse en la información comparada elaborada por la Secretaría de la Red Iberoamericana, labor que desarrolla esta AEPD.

Por lo que se refiere a los Estados Unidos, desde la aprobación de la CAN SPAM ACT en 2003 por la que se establecieron claras normas de protección de la privacidad en las comunicaciones comerciales electrónicas y se encomendó dicha misión a la Comisión Federal del Comercio de los US (FTC), la tendencia a incrementar y hacer efectiva esta protección ha sido creciente. En el año 2006 se ha producido un nuevo desarrollo normativo que favorece una cooperación internacional efectiva con otras autoridades de protección de datos, la SAFE WEB ACT, ya que permite a la FTC mantener la confidencialidad de la información facilitada por otra autoridad en el curso de investigaciones relacionadas con infracciones de privacidad en telecomunicaciones.

I. EUROPA

ACTIVIDAD DERIVADA DE LA DIRECTIVA EUROPEA DE PROTECCIÓN DE DATOS: EL GRUPO DE TRABAJO DEL ARTÍCULO 29

El Grupo de Trabajo del Artículo 29 (en adelante GT29), creado por la Directiva 95/46/CE tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

El GT 29 se reúne en plenarios con una periodicidad bimensual y se organiza en diversos subgrupos de trabajo para analizar todas aquellas cuestiones que inciden, o pueden llegar a afectar, a la protección de datos personales. El GT 29 emite sus observaciones a través de Decisiones, Dictámenes, Documentos de Trabajo, Informes o Recomendaciones.

Uno de los temas de los que el GT29 se ha ocupado repetidamente desde el año 2002 ha sido la transferencia de datos de pasajeros con destino a los Estados Unidos, el asunto PNR. En 2006 la evolución ha sido la siguiente:

El 30 de mayo de 2006, el Tribunal de Justicia de la Unión Europea emitió la sentencia por la que se resolvía los dos recursos de anulación presentados por el Parlamento Europeo en julio de 2004. Los recursos argumentaban la anulabilidad tanto de la Decisión de la Comisión Europea declarando el nivel adecuado de protección de datos de EEUU como de la Decisión sobre el Acuerdo Internacional firmado con las autoridades americanas para dotar de base legal a la transmisión de datos PNR de los pasajeros. Ambos recursos fueron presentados individualmente pero fueron acumulados por el Tribunal de Justicia, que estimó, por defecto de forma, los dos recursos y ordenó la denuncia del acuerdo con EEUU.

En junio de 2006, el GT 29 aprobó una opinión en la que ponía de manifiesto los principales elementos de preocupación que surgían tras esta nueva situación, en la que a partir del 30 de septiembre de 2006, fecha límite en la que el Acuerdo debía ser denunciado, las transmisiones de datos por parte de las aerolíneas dejaban de tener base legal. Los principales aspectos señalados por la opinión fueron:

- Los acuerdos bilaterales entre EEUU y los Estados miembros de la UE deben evitarse.
- Todo nuevo acuerdo debe, al menos, preservar e integrar el actual nivel de protección de los datos tal y como se recoge en los compromisos de EEUU de 2004 y tener en cuenta las consideraciones críticas hechas públicas por el GT 29 en sus opiniones previas sobre PNR, incluyendo la cuestión de la reducción de datos.
- El sistema "push", por el que los datos son enviados en vez de permitir el acceso a los sistemas de reserva (sistema "pull"), es el que debe ser implementado.
- Es necesaria la limitación estricta de la finalidad para la transmisión que se haga a partir de ahora de datos PNR.
- El GT29 espera que el mecanismo de una revisión conjunta anual se mantenga, en línea con el actual acuerdo.

Otro asunto importante referido a las relaciones transatlánticas que ha sido objeto de especial atención por parte del GT29 durante el año 2006 es el conocido como caso SWIFT.

En junio de 2006 diversas informaciones en los medios de comunicación desvelan la existencia de un programa por el que el Gobierno de EEUU ha tenido acceso a los datos

relativos a transferencias bancarias internacionales realizadas a través de la Sociedad SWIFT en el marco de la lucha contra el terrorismo. Asimismo, una denuncia fue formalmente presentada ante las autoridades de protección de datos de 33 países, entre ellos España, con vistas a destapar un caso en el que la privacidad de los ciudadanos europeos se veía seriamente dañada. SWIFT es una sociedad cooperativa con sede en Bélgica, cuyo Derecho le es de aplicación, pero tiene oficinas, que se desvelaron de carácter puramente comercial, en otros países, entre ellos España. Es por ello que la AEPD ha participado activamente en la investigación de los hechos denunciados, pero ello en el marco de las actuaciones de inspección realizadas por la autoridad belga, competente en este caso.

El GT 29, por su parte, aprobó una opinión en la que se estableció tanto la responsabilidad de SWIFT como de las instituciones financieras que utilizan sus servicios en la transmisión de los datos a EEUU para una finalidad distinta de para la que fueron recabados. Y ello porque, mientras los datos eran recogidos por los bancos con vistas a realizar la transferencia solicitada por los clientes, esa información era posteriormente enviada al Departamento del Tesoro de EEUU que la podía utilizar en su lucha contra el terrorismo.

Asimismo, el GT 29 instaba a SWIFT a cesar esa transferencia ilegal de datos, máxime cuando los clientes de las entidades financieras ni siquiera tenían información de que la transmisión de los datos se estuviera produciendo.

Una cuestión de especial relevancia analizada en 2006 por el GT 29 ha sido la retención de datos en las comunicaciones electrónicas.

Como ya mencionamos en las memorias de la Agencia Española de Protección de Datos de 2004 y 2005, la cuestión de la retención de datos de las comunicaciones electrónicas ha estado situada al más alto nivel en la agenda política europea hasta la adopción final de la Directiva 2006/24 CE de 15 de marzo de 2006. En marzo de 2006, el GT 29 aprobó una nueva opinión con la que reaccionaba a la aprobación formal de la Directiva. En la misma, se reiteraban las garantías que debían ser adoptadas para evitar la vulneración de los derechos fundamentales de los ciudadanos y se instaba a las autoridades nacionales a desarrollar un papel activo en la defensa de los mismos en los procesos de transposición interna de la Directiva. En definitiva, las autoridades volvieron a señalar los siguientes elementos de preocupación:

- Toda restricción al derecho fundamental a la confidencialidad de las comunicaciones, debe estar justificada por una necesidad apremiante, sólo debe permitirse en casos excepcionales y deberá contar con las garantías adecuadas. La finalidad debe ser la lucha contra el terrorismo y la delincuencia organizada, dejando atrás términos excesivamente ambiguos.
- El acceso a los datos deberá ser autorizado caso por caso por una autoridad judicial, sin perjuicio de aquellos países en los que sea posible el acceso autorizado por ley y bajo una supervisión independiente. Los destinatarios de la información debe ser únicamente las autoridades policiales específicamente designadas.

- Los sistemas de almacenamiento de estos datos deberán estar separados de aquellos sistemas que las compañías utilicen a efectos empresariales y deberán estar sometidos a unas medidas de seguridad más rigurosas.

Otros asuntos de interés examinados por el GT29 se refieren a las siguientes materias:

■ LOS FICHEROS CREADOS EN APLICACIÓN DE LA LEY SARBANES-OXLEY

En virtud de esta ley norteamericana los Comités de Auditoría de las empresas que cotizan en la Bolsa de Nueva York deben dar curso a todas aquellas informaciones de sus empleados que denuncien casos de corrupción o malas prácticas en la empresa. A los efectos de protección de datos esto supone la creación de ficheros con información sobre posibles vulneraciones de la legalidad por parte de los trabajadores de una empresa (ficheros de integridad).

El GT 29 analizó las implicaciones de estos ficheros en su Dictamen 1/2006 y puso de relieve que el establecimiento de estos sistemas debían hacerse de acuerdo con los principios establecidos en la Directiva 95/46/CE, garantizando el derecho fundamental a la protección de datos personales, tanto respecto del denunciante como del denunciado.

■ FILTRACIÓN DE CORREO ELECTRÓNICO

Consciente de la expansión de los distintos servicios de comunicación en línea -como los servicios de correo electrónico gratuitos de la red- en febrero de 2006, el GT 29 adoptó el "Dictamen 2/2006 del Grupo de trabajo 29 sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico" en el que examina las disposiciones sobre confidencialidad de las comunicaciones electrónicas previstas en la Directiva 2002/58 CE sobre la privacidad en las telecomunicaciones, transpuesta a la legislación española en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Tanto los proveedores de servicios de Internet, como los prestadores de servicios de correo electrónico llevan a cabo una práctica habitual de inspección y filtración de las comunicaciones con el fin de eliminar el correo masivo no solicitado, virus, así como la detectar contenidos concretos.

El principal objetivo de este documento es servir de guía para que estas prácticas se lleven a cabo respetando la intimidad de las comunicaciones por correo electrónico y, más en concreto, en el del filtrado de las comunicaciones en línea, estableciendo, por ejemplo, la obligación de informar a los abonados sobre el tratamiento de sus datos personales.

■ E-CALL

El servicio e-call supone un servicio paneuropeo de llamada desde el vehículo que utiliza el número de llamada de urgencia europeo 112 en caso de accidente, y que se crea bajo la iniciativa "eSafety" en una Comunicación de la Comisión del año 2002.

A fin de responder a las cuestiones relativas a la intimidad y la protección de datos que plantea el despliegue de este sistema, se consideró necesario el análisis de la situación, por lo que el GT 29 aprobó el "Documento de trabajo sobre la protección de datos y las consecuencias para la intimidad en la iniciativa eCall". El objetivo del presente documento de trabajo se enfoca a exponer las preocupaciones que en materia de protección de datos y derecho a la intimidad suscitan estos servicios, recomendando su posible introducción con carácter voluntario.

■ REVISIÓN DEL PAQUETE REGULADOR DE TELECOMUNICACIONES

En contestación a la Consulta Pública que realizó la Comisión Europea concerniente al paquete regulador de las Directivas de Telecomunicaciones, entre las que se encuentra la Directiva 2002/58/CE de privacidad en las comunicaciones, el GT 29 contribuyó con la aprobación del "Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas", en el que se aportaban una serie de observaciones, tanto generales, en torno al tratamiento de los datos personales que se realizan en comunicaciones electrónicas o a través de las mismas, como específicas, sugiriendo, por ejemplo, que se abordaran en la Directiva temas relacionados con las aplicaciones en línea, entre los que se incluyen cuestiones de seguridad o la responsabilidad de los operadores, así como una aclaración de la personalidad jurídica tanto de los proveedores de infraestructuras de acceso y de los proveedores de servicios como de los responsables del tratamiento de los datos. Además, el GT 29, propone la mejora de las medidas de seguridad, pero no apoya ninguna medida que lleve o pueda llevar a incrementar la vigilancia o a bloquear los contenidos.

■ DIRECTORIOS WHOIS

Los directorios Whols permiten obtener acceso público e información sobre direcciones IP y nombres de dominio registrados, con la finalidad de facilitar información en caso de incidentes informáticos y así contactar con el responsable técnico de otra red o de otro dominio. No obstante, este servicio puede asimismo ser utilizado por un potencial atacante con el fin de recabar información y enviarle spam. Debido a los problemas que de forma intrínseca plantean este tipo de sistemas, los directorios Whols ya habían sido analizados con anterioridad por el GT 29 en el dictamen 2/2003 (WP 76), en el que se examinaban los aspectos jurídicos que se plantean cuando son los particulares los que registran nombres de dominio y estos no son los mismos que las empresas u otras personas jurídicas las que lo hacen.

La AEPD, que tiene la competencia de investigación en materia de lucha contra el spam, ha participado en los debates que han surgido en el seno del Governmental Advisory

Committee, que asesora a ICANN (Internet Corporation for Assigned Names and Numbers) en el que se han dado unas pautas para la utilización de los servicios globales de Whols. Durante el año 2006, los debates han estado centrados en la publicidad o no de todos los datos Whols puesto que, si bien entre las finalidades iniciales de estos directorios no estaba contemplada la investigación, en muchas ocasiones estos servicios suponen la base para la averiguación de un delito y son utilizados por las autoridades competentes. Por otro lado, la publicación de estos datos puede provocar una invasión en la esfera privada del individuo, debiendo estos directorios de observar las disposiciones que en materia de protección de datos establece no sólo la Directiva, sino también las distintas leyes nacionales, que recogen principios como la finalidad.

La AEPD, en línea con el GT 29, ha defendido en estas reuniones, que si bien existe la necesidad de acceso a estos datos por parte de las autoridades competentes, de esta no subyace la exigencia de un acceso online, por lo que la solución ideal sería un acceso por niveles o privilegios a estas bases de datos, tal y como se hace en Reino Unido y Francia.

■ DATOS DE SALUD

El GT 29 ha venido trabajando en los últimos dos años en aportar directrices de protección de datos que se tengan en cuenta al regular la incorporación de las historias clínicas a soportes electrónicos, ya que este sistema de historia clínica electrónica se está generalizando en todos los Estados Miembros.

Al cierre de esta Memoria se ha aprobado el documento de trabajo que se ha sometido a consulta pública y que puede encontrarse en la página web del GT 29.

■ ENFORCEMENT TASK FORCE

El primer informe sobre la implementación de la Directiva 95/46/CE (mayo de 2003) puso de manifiesto un déficit de capacidad efectiva para hacer cumplir la ley (enforcement) en varios Estados Miembros e importantes carencias en la función supervisora de algunas autoridades. En este contexto el GT 29 acordó realizar una actuación coordinada, emprendida por todas las Autoridades de los Estados Miembros, y que se planificaría en el marco del subgrupo de trabajo de Enforcement Task Force. Este subgrupo analiza la capacidad de aplicar y ejecutar las normas de protección de datos por parte de las Autoridades supervisoras y se crea a raíz de la "Declaración del Grupo del artículo 29 sobre el control de la aplicación de la legislación", del 25 de noviembre de 2004.

La actuación sincronizada se dirige al sector del seguro privado de salud, y se centra en el análisis de la información obtenida a través de un cuestionario común que se cumplimentará por las compañías seleccionadas en todos los Estados Miembros. Durante el año 2006, con las respuestas al cuestionario, las autoridades de protección de datos elaboraron un informe nacional en el que se analizaban los resultados obtenidos. La AEPD ha contribuido de manera especial en todas las fases de esta actuación conjunta dada su amplia experiencia en inspecciones sectoriales.

PROPUESTAS LEGISLATIVAS RELEVANTES

A continuación se recogen las novedades normativas más importantes en el ámbito comunitario:

PROPUESTA DE MODIFICACIÓN DEL PAQUETE DE DIRECTIVAS DE TELECOMUNICACIONES

En junio del año 2006, la Comisión Europea aprobó una Comunicación en relación con la revisión que se ha llevado a cabo del marco regulador de las telecomunicaciones (SEC (2006) 81). En esta comunicación se informaba sobre el funcionamiento del paquete de directivas que regulan las redes y servicios de comunicaciones electrónicas, y se identifican áreas en las que es necesario introducir algún cambio.

La Comunicación se complementaba con un Documento de Trabajo de los servicios de la Comisión ("Comission Staff Working Document"), que establece en mayor detalle los posibles cambios al marco regulador y un documento de Valoración del Impacto ("Impact Assesment"). En estos dos documentos se recogen las conclusiones de las aportaciones realizadas por los agentes implicados.

Con todas las aportaciones, la Comisión elaboraría propuestas legislativas para la modificación del marco regulador, y que se presentarán al Parlamento Europeo y al Consejo.

El actual marco europeo de las comunicaciones electrónicas está formado por un paquete de 5 Directivas relativas a los servicios de comunicación que se transfieren electrónicamente, por tecnología wireless o fija, por datos o por voz, basada en Internet o en circuito cerrado, empresarial o personal. Estas normas europeas están creadas para estimular la competencia y crear oportunidades para las nuevas compañías. Pretenden una reducción de precios y a una gama más amplia de productos y de servicios para el consumidor. Este marco normativo entró en vigor en el año 2002 teniendo que ser transpuesto en los Estados miembros antes de julio de 2003. Las Directivas son las siguientes:

- Directiva 2002/19/CE de 7 de marzo de 2002 relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso).
- Directiva 2002/20/CE de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización).
- Directiva 2002/21/CE de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónica (Directiva marco).

- Directiva 2002/22/CE de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).
- Directiva 2002/58/CE de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Es precisamente respecto a esta última, la denominada Directiva de privacidad en las telecomunicaciones, sobre la que se proponen los cambios que a continuación se resumen:

- Mejora de los mecanismos de aplicación previstos en el marco regulador,
- Seguridad,
- Obligación de adoptar medidas de seguridad y concesión de competencias a las Autoridades nacionales de regulación para que puedan determinar y controlar la aplicación técnica, y
- Notificación de las violaciones de la seguridad por los operadores de la red y los proveedores de servicios de Internet.

Como se avanzaba en el punto relativo al trabajo llevado a cabo por el Grupo de Trabajo del Artículo 29, este contestó a la Consulta pública con el fin de interpretar y desarrollar los cambios propuestos a la Directiva 2002/58/CE de privacidad en las comunicaciones.

Las observaciones del GT 29, así como toda la documentación relativa a la consulta pública llevada a cabo por la Dirección General de la Sociedad de la Información está disponible en el siguiente hipervínculo:

http://ec.europa.eu/information_society/policy/ecommm/info_centre/documentation/public_consult/index_en.htm#communication_review

EL TRATADO DE PRÜM

El Tratado de Prüm, firmado en la ciudad alemana del mismo nombre en mayo de 2005, tiene como objetivos la profundización de la cooperación fronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la inmigración ilegal. Los actuales países signatarios son Bélgica, Holanda, Luxemburgo, Francia, España, Alemania y Austria (siendo estos dos últimos los únicos que ya han completado el proceso de ratificación del Tratado), pero ya han mostrado su interés en participar en el mismo Italia, Finlandia, Portugal y Polonia.

El Tratado prevé el intercambio de datos de ADN, huellas dactilares, matriculación de vehículos y otros datos que pudieran ser ulteriormente necesitados con vistas al cumplimiento de los fines del Tratado. Respecto de los datos de ADN se deberán crear índices de referencia sobre los datos contenidos en los ficheros de análisis de ADN nacionales a los que podrán acceder de forma automatizada las otras partes contratantes. La consulta de índices de referencia se realizará sólo para casos concretos y de acuerdo con el Derecho de la parte que realice la consulta. En caso de concordancia, la transmisión de otros datos de carácter personal se hará de acuerdo con el derecho interno de la parte requerida y siguiendo los mecanismos de cooperación policial previstos en el Tratado de la Unión Europea. Las consultas automatizadas de los datos de huellas dactilares también se harán a través del acceso a índices de referencia.

Otras disposiciones del Tratado se refieren a:

- Medidas para la prevención de atentados terroristas: se prevé la transmisión de datos, sin que medie petición previa, cuando existan hechos que justifiquen la presunción de que la persona en cuestión vaya a cometer alguno de los delitos contenidos en la Decisión Marco de lucha contra el terrorismo.
- Medidas contra la migración ilegal: incluyendo la organización de vuelos conjuntos de repatriación.
- Asistencia en caso de catástrofes, accidentes graves y grandes eventos de carácter transfronterizo, así como otras formas de intervención conjunta.

El Tratado recoge, en un capítulo específico, unas pautas para la protección de los datos manejados en el curso de la aplicación del Tratado cuyos rasgos más destacados son: un nivel mínimo de protección fijado en el Convenio 108 del Consejo de Europa, limitación estricta del principio de finalidad, cancelación de los datos una vez haya desaparecido la finalidad de la transmisión, acceso a los datos a través de un único punto de contacto nacional, así como el reconocimiento al titular de los datos de los derechos de acceso, rectificación y cancelación y de acudir a un Tribunal o a una autoridad de control independiente en caso de vulneración de los derechos.

Por su parte, la AEPD ha participado en diversas reuniones a nivel europeo con vistas a hacer valer los principales elementos de preocupación detectados en este Tratado, sobre todo relativos a las necesarias salvaguardias que deben adoptarse en lo que a la transmisión de datos de ADN se refiere y el escrupuloso cumplimiento del principio de finalidad.

MODIFICACIÓN DE LA BASE JURÍDICA DE EUROPOL

El 20 de diciembre de 2006 fue presentada la propuesta de Decisión del Consejo por la que se crea la Oficina Europea de Policía (EUROPOL) (COM(2006) 817). La idea que subyace de la modificación de la base jurídica por la que se regula Europol es

la necesidad de dotarle de nuevas competencias que le permitan hacer frente a las demandas en materia de seguridad en el marco de la coordinación y colaboración entre Estados miembros. Esta necesidad de ir adecuando la actividad de Europol a las materias en el ámbito de la cooperación policial que vayan manifestándose como imprescindibles hace necesario dotar a Europol de un instrumento de adaptación y funcionamiento ágil que evite procedimientos extremadamente complejos que dificulten su actuación.

El Convenio Europol, aprobado en 1995, ha sido objeto de modificación hasta el momento por tres protocolos, ninguno de los cuales está aún en vigor, y ello precisamente por la necesidad de que sean ratificados por todos los Estados miembros. Una lentitud en la tramitación que obstaculiza en gran medida la eficacia de la labor de Europol.

La propuesta de Decisión, actualmente en fase de tramitación en la que se contará con la intervención del Parlamento Europeo, ha sido también abordada por la Autoridad Común de Control de Europol, que el 5 de marzo de 2007 aprobó una opinión cuyos elementos más esenciales son:

- El proyecto distingue entre los objetivos de Europol-apoyar y reforzar la cooperación entre Estados Miembros para la lucha contra el terrorismo y los delitos graves- y las competencias de Europol, que quedan limitadas a los casos que afecten a dos o más Estados Miembros. En juicio de la ACC el objeto de esta distinción debe clarificarse, así como las consecuencias que pueda conllevar para las estructuras de información de Europol.
- El tratamiento por Europol de datos puestos a disposición por entidades públicas y privadas debe hacerse bajo la condición de que las solicitudes de información se dirijan a las unidades nacionales, que examinarán la solicitud.
- Deben especificarse las diferentes responsabilidades de Europol en materia de protección de datos cuando el tratamiento de los datos tenga lugar fuera de sus instalaciones (en el seno de equipos conjuntos de investigación).
- El texto de la Decisión debe mencionar la finalidad del Sistema de Información Europol, así como la necesidad de consultar la ACC.
- También se debe introducir la obligación de consultar la Autoridad Común de Control y otras Autoridades de Supervisión afectadas antes de que se adopte cualquier decisión relativa a la interconexión del sistema de información de Europol con otros sistemas.
- Se debe realizar una revisión anual de los datos contenidos en los ficheros de análisis.
- La comunicación de datos a órganos terceros debe contar con un procedimiento de consulta a la ACC.

- El derecho de acceso debe garantizarse, debiendo Europol responder a la solicitud en un plazo breve.

ACTIVIDAD DERIVADA DE LOS CONVENIOS DE EUROPOL, SCHENGEN , SISTEMA DE INFORMACIÓN ADUANERO Y EUROJUST

La Autoridad Común de Control (ACC) de Schengen mantuvo a lo largo de 2006, continuados debates sobre la modificación de la base jurídica del Sistema de Información Schengen (SIS). A las opiniones que ya se aprobaron cuando la propuesta fue presentada en 2005 se unió otra opinión a probada en septiembre de 2006 que incidía sobre los elementos de preocupación que se iban poniendo de manifiesto a medida que avanzaban las negociaciones en el Consejo. Estos aspectos preocupantes eran, principalmente, el acceso al SIS por parte de los servicios secretos de los Estados miembros, la supervisión del sistema una vez que desaparezca la ACC tras la entrada en vigor del nuevo SIS y el acceso a la información por parte de EUROPOL.

Por su parte, la ACC de Europol organizó el 17 de octubre una Conferencia en la que se pretendía abordar el futuro de la Oficina Europea de Policía, sobre todo en el marco de la posible modificación de su base jurídica - lo que se materializó con la propuesta de 20 de diciembre de 2006 expuesta anteriormente-. En esta Conferencia se puso de manifiesto que toda nueva atribución de competencias a Europol debía estar unida al establecimiento de nuevas medidas para proteger los datos que sean objeto de tratamiento. Asimismo, Europol debía seguir siendo objeto de inspecciones periódicas por parte de las Autoridades de control con vistas a salvaguardar que tanto los ficheros de análisis como el Sistema de Información Europol contaban con un sistema adecuado de garantías.

Por último, la AEPD ha colaborado durante el 2006 en la inspección del sistema central Eurodac que está llevando a cabo el Supervisor Europeo de Protección de Datos, responsable del sistema. Esta colaboración se ha materializado a través del envío de información sobre los mecanismos de obtención de las huellas dactilares de los solicitantes de asilo o extranjeros detectados en situación irregular en España así como su transmisión al sistema central.

OTRAS ACTIVIDADES EN EL MARCO EL TERCER PILAR

La AEPD participa activamente en las reuniones del denominado Grupo de Trabajo de Policía que, en el marco del mandato otorgado anualmente por la Conferencia de Primavera, centra sus debates en las propuestas legislativas en curso sobre el tratamiento de datos con fines policiales. Durante el año 2006, el Grupo de Trabajo de Policía ha debatido sobre el concepto de disponibilidad, utilizado para describir el

marco en el que se debe producir el intercambio de información entre las fuerzas del orden público. Y ello por cuanto las últimas propuestas legislativas ya incluyen en su texto que toda información en manos por la policía de un Estado Miembro debe poder estar disponible para sus homólogos de otro Estado Miembro. Los mecanismos en que se articula esta disponibilidad y las garantías que deben proteger esa información han sido debatidas por las autoridades de protección de datos que han puesto reiteradamente de manifiesto que el intercambio de información no puede derivar, en ningún momento en una disminución en las garantías de protección de los datos personales de los ciudadanos.

ACTIVIDAD DERIVADA DEL CONVENIO 108 DEL CONSEJO DE EUROPA

La Agencia Española de Protección de Datos participa en el Comité Consultivo (T-PD) establecido en el artículo 18 del Convenio para la protección de las personas físicas en relación con el tratamiento automatizado de datos personales (Convenio 108). El citado Comité celebró su reunión plenaria número 22 los días 8 a 10 de marzo de 2006.

En dicha reunión se repasó la actividad llevada a cabo por el Consejo de Europa y se adoptaron las futuras líneas de actuación del Comité.

Así, a partir de la adopción en 2005 del informe definitivo sobre "La autodeterminación informativa en los tiempos de Internet", que analiza los riesgos que para la privacidad tienen las redes de telecomunicaciones y el equilibrio de intereses entre quienes tienen que tratar esas informaciones y los titulares de la misma, se encomendó al Bureau del comité Consultivo (T-PD-BUR), en su condición de órgano de preparación y discusión previa de los documentos que se someten posteriormente al plenario, la elaboración de un documento que estableciera los principios básicos para la determinación de los conceptos de tratamiento automatizado y responsable del tratamiento en el marco de las redes globales de telecomunicaciones. Del mismo, se acordó la realización de distintos documentos con la aplicación de los criterios de adecuación en materia de transferencias internacionales de datos, tomando en consideración los trabajos llevados a cabo en el seno de la OCDE, y los tratamientos que implican el establecimiento de perfiles.

Por otra parte, se continuaron los trabajos, iniciados durante el año anterior, en relación con la propuesta de formalización del derecho a la protección de datos como derecho fundamental (que se ha declarado autónomo en algunos países como España y Portugal) mediante un instrumento propio del Consejo de Europa para garantizar el acceso al Tribunal Europeo de Derechos Humanos (TEDH), tomando esencialmente en consideración el análisis ya realizado de la jurisprudencia del Tribunal en esta materia.

Igualmente, durante la reunión del plenario, fueron objeto de debate cuestiones relacionadas con la aplicación de los principios del Convenio 108 al tratamiento de datos biométricos, tomando en consideración el informe elaborado sobre esta materia y sometido al plenario en el año 2005, así como las implicaciones que para el derecho fundamental a la protección de datos revise la lucha contra el terrorismo.

Por último, el Comité ofreció todo su apoyo para la efectiva implantación del día europeo de la protección de datos, finalmente establecido el día 28 de enero, en conmemoración de la adopción del Convenio 108.

RELACIONES BILATERALES EN EL ÁMBITO EUROPEO

Del mismo modo se mantienen en 2006 las tradicionales relaciones con la Autoridad de Protección de Datos de Portugal, con la que la AEPD se reunió en dos ocasiones a lo largo del año 2006. En la primera de las reuniones, celebrada en enero en San Lorenzo de El Escorial, y como continuación de los trabajos llevados a cabo en el anterior encuentro, se compararon las visiones de ambas autoridades respecto a la utilización de datos para estudios de investigación científica y ensayos clínicos. Además, se trabajó sobre las experiencias de ambas delegaciones en relación con los tratamientos realizados en aplicación de la Ley Sarbanes-Oxley, y contrastando los avances que los respectivos países han tenido en su administración electrónica.

En el segundo de los encuentros, celebrado en Óbidos (Portugal) en diciembre de 2006, se debatieron los flujos internacionales de datos, concluyendo ambas autoridades que es necesario encontrar formas flexibles que se adapten a la creciente circulación de información y de prestación de servicios, que han de mantener un nivel adecuado de protección de datos.

Además, durante el encuentro, ambas autoridades compartieron sus visiones respecto a la seguridad en los mercados financieros y las "líneas de integridad" para las empresas que cotizan en la Bolsa de Nueva York coincidiendo en la necesidad de notificación, fundamento jurídico, así como el necesario cumplimiento con los derechos de los trabajadores.

A lo largo de 2006 la AEPD ha participado en el proyecto Twinning Light que ha desarrollado la República Checa en Bosnia-Herzegovina.

Asimismo, dentro de la línea de colaboración permanente de la AEPD con la Comisión Europea, y con el fin de apoyar el proceso de ampliación de la UE y cooperar en la consolidación de instituciones y mecanismos de protección de datos en los nuevos Estados Miembros, la AEPD participó en el seminario organizado en el mes de octubre por la Dirección General de Ampliación de la Comisión Europea a través de TAIEX (Instrumento de Asistencia Técnica e Intercambios de Información) en la nueva República de Montenegro, independiente desde mayo de ese mismo año y país candidato a incorporarse a la UE.

El seminario en el que, junto con representantes de varias autoridades europeas de protección de datos participaban también representantes de la Comisión Europea, se dirigía a responsables de los Ministerios de Telecomunicaciones, Interior, Justicia y Empleo de esa nueva República y su objetivo era proporcionar información y asistencia en

materia de protección de datos de cara a una eventual incorporación de Montenegro a la Unión Europea.

II. IBEROAMERICA

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

La Red Iberoamericana de Protección de datos se creó en junio de 2003, con ocasión de la celebración del II Encuentro Iberoamericano de Protección de Datos, que tuvo lugar en La Antigua (Guatemala), que contó con la participación de 15 de los entonces 21 Estados que conformaban la Comunidad Iberoamericana (actualmente la Comunidad Iberoamericana está integrada por 22 Estados, tras la reciente incorporación de Andorra). Los participantes, en la Declaración firmada al finalizar el Encuentro, resaltaron la necesidad de dotar de una estructura permanente a este foro con el objeto de reforzar la mutua y continua colaboración entre todos y de abrirla a la incorporación de representantes de todos los países Iberoamericanos.

Por ello la Red se crea como un foro permanente cuyo objetivo es potenciar las iniciativas de intercambio de experiencia entre los países iberoamericanos, estableciendo canales siempre abiertos de diálogo y colaboración en materia de protección de datos. La Secretaría de la Red la ostenta la Agencia Española de Protección de Datos que proporciona el soporte organizativo a este foro de dialogo. La Red cuenta con representación de entidades de 19 países de los 22 que integran la Comunidad Iberoamericana. Entre los objetivos de la Red, destaca especialmente su labor tendente a impulsar la elaboración de los instrumentos normativos necesarios para garantizar este importante derecho fundamental en aquellos países de la Comunidad Iberoamericana en los que aún no se ha emprendido esta regulación.

En mayo de 2006, la AEPD, en colaboración con la Agencia Española de Cooperación Internacional y la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas, reunió en Santa Cruz de la Sierra, Bolivia, a representantes de 12 países miembros la Red Iberoamericana de Protección de Datos.

Durante el encuentro los participantes, que se reunieron en los cuatro grupos de trabajo creados en el IV Encuentro Iberoamericano de protección de datos, celebrado en México en 2005, sobre "Impulso Normativo y Armonización", "La Red On-line" "Instrumentos de Autorregulación" y "Tratamientos de Datos de Salud", elaboraron distintos documentos de trabajo que serán sometidos a aprobación en el próximo encuentro de la Red que se celebrará en el primer semestre de 2007.

Entre las principales conclusiones recogidas en dichos documentos destacan:

- Es necesario adoptar medidas que garanticen un nivel de protección adecuado en todos los países iberoamericanos con el objetivo de que exista una armonización normativa entre los Estados que permita el flujo de información necesario para el correcto desarrollo del mercado. En este sentido, se asumió el compromiso de elaborar una propuesta de directrices para la armonización de la regulación de la protección de datos en la comunidad Iberoamericana, y colaborar mediante el asesoramiento con los países que adopten iniciativas legislativas en este ámbito.
- La finalidad principal de la historia clínica debe ser el de facilitar la asistencia sanitaria de forma que consten en ella todos aquellos datos que permitan un conocimiento veraz y actualizado del estado de salud. La obtención, uso, archivo, custodia y transmisión de los datos de salud contenidos en ella exigen instrumentos adicionales de garantía y deben responder a principios básicos tales como el respeto a la dignidad de la persona, la autonomía de su voluntad y su intimidad, y la protección de los datos personales. No obstante, el principio básico del consentimiento de la persona puede verse limitado cuando tal limitación constituya una medida necesaria por razones de interés general reconocidas en una norma con rango de Ley. Asimismo, se concluyó que los sistemas sanitarios han de prever garantías de movilidad mediante el establecimiento de sistemas de intercambio de información de salud entre los distintos organismos, centros y servicios del sistema sanitario, que garanticen la adecuada asistencia sanitaria cuando los ciudadanos se desplacen por el territorio nacional.
- Las iniciativas de autorregulación, entendidas como complemento a un marco normativo previamente definido por el Estado, pueden ofrecer un valor añadido en la protección de datos personales. Estos mecanismos pueden añadir garantías adicionales a las contempladas en las regulaciones, contribuir a la consolidación de una cultura de protección de datos y fomentar el tratamiento correcto de la información personal en la medida en que aporten un valor añadido y tengan efectividad práctica. Es por ello que se recomienda la incorporación en los textos legales sobre protección de datos de disposiciones explícitas tendentes a utilizar mecanismos de autorregulación, la promoción de su publicidad, y el establecimiento de medidas efectivas en caso de incumplimiento de estas normas.
- Por último, la dispersión geográfica de los miembros de la Red hace preciso dotarla de mecanismos ágiles y eficaces para mantener la fluidez en este intercambio de experiencias e informaciones. Por este motivo, durante la celebración del Seminario Iberoamericano fue presentado el proyecto de la Red "on line". El objetivo principal de este proyecto es contar con un instrumento virtual de la Red Iberoamericana en el desarrollo y la divulgación de sus actividades, la difusión del derecho fundamental a la protección de datos en Iberoamérica y configurar un sistema de intercambio de información entre sus miembros.

III. ESTADOS UNIDOS

COOPERACIÓN CON LA COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS

La Agencia viene desarrollando desde el año 2005 una cooperación efectiva con la Comisión Federal del Comercio (FTC) de los Estados Unidos, entidad competente para luchar contra los fraudes a los consumidores y las violaciones de las normas sobre comunicaciones comerciales electrónicas. La existencia de ámbitos comunes de actuación y la similitud de métodos y facultades para conseguir el cumplimiento de la ley hicieron posible la firma de un Acuerdo de Entendimiento entre ambos organismos.

Una aplicación esencial y práctica del mismo es la difusión de las normas de privacidad y protección de datos en los foros académicos universitarios de los respectivos países. Durante el otoño de 2006, representantes de la Agencia y de la FTC impartieron en la Facultad de Derecho de la Universidad de Georgetown (Washington DC) un seminario de derecho comparado sobre la protección de datos en ambos lados del Atlántico. Su objetivo no es solo comparar los modelos normativos europeo y americano sino también explicar a los futuros profesionales del derecho en los Estados Unidos, los métodos de trabajo que utilizan las autoridades de supervisión para hacer cumplir las normas de protección de datos y cómo pueden cooperar mutuamente.

IV. OTRAS ACTIVIDADES INTERNACIONALES

CONFERENCIAS INTERNACIONALES DE PROTECCIÓN DE DATOS

Los días 24 y 25 de abril de 2006 tuvo lugar en Budapest la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos. Esta Conferencia se celebra anualmente en Europa y tiene como finalidad el análisis de todas aquellas cuestiones, legislativas o tecnológicas, que puedan afectar a la privacidad de los ciudadanos europeos con el objetivo de buscar soluciones armonizadas en dicho ámbito.

En su reunión de 2006 se abordaron temas como la tecnología de identificación por radiofrecuencia (RFID), las denominadas "líneas de integridad" puestas actualmente en marcha en numerosas empresas o la centralización de la información sanitaria y la tarjeta sanitaria electrónica. Como también viene siendo habitual en las últimas conferencias europeas, las autoridades de protección de datos debatieron sobre el tratamiento de datos de carácter personal por las fuerzas de seguridad pública, a cuyos efectos

aprobaron una declaración de aplicación al tratamiento de datos en el III Pilar. En la misma, se hizo hincapié en que la utilización de la información disponible para las fuerzas policiales de los Estados Miembros, así como el intercambio de la misma debería realizarse en el marco de unos estándares mínimos que garantizaran la protección de los datos personales de los ciudadanos. Es partiendo de esta premisa con la que se debe lograr un equilibrio entre la utilización de la información como medio valioso de las autoridades policiales y judiciales y la protección de los derechos fundamentales, y entre ellos a la protección de sus datos personales, de los ciudadanos de la Unión Europea.

En otoño se celebró en Londres la Conferencia Internacional de Protección de Datos y su organización corrió a cargo de la Comisión de Protección de Datos de Reino Unido (Information Commission Office). La Conferencia, cuyo tema central giró en torno al tema "Una sociedad bajo vigilancia", contó con la participación en torno a diferentes paneles, de representantes de las autoridades de protección de datos del ámbito internacional, parlamentarios, y representantes de medios de comunicación, universidad y de ONGs.

Resultado de esta reunión nace la "London Initiative", una iniciativa de la CNIL, la Autoridad de Protección de Datos francesa, que a través de su documento "Claves para la comunicación de la protección de datos y como incrementar su eficacia" enfatiza la importancia de la privacidad y la protección de los datos personales en los rápidos desarrollos, y la necesidad de una acción urgente para afrontar los nuevos desafíos. Mediante la adhesión a esta iniciativa, en la que la AEPD forma parte, las autoridades de protección de datos se comprometen a:

- Desarrollar actividades de comunicación.
- Adaptar sus prácticas y métodos mediante la evaluación minuciosa de su eficacia y efectividad.
- Contribuir al reconocimiento institucional de las Autoridades de Protección de Datos a nivel internacional y fomentar la participación de otras partes interesadas apropiadas, nacional e internacionalmente.

Además, los Comisarios de Privacidad y Protección de Datos presentes, aprobaron la Acreditación de 8 nuevos miembros para la Conferencia y se aprobaron dos resoluciones sobre cuestiones organizativas y sobre la protección de la privacidad y los buscadores de Internet.

Previamente, con motivo de esta reunión internacional, se celebraron dos reuniones sobre "Security breaches" y "Cooperación Internacional en materia de Enforcement" respectivamente, organizadas por sectores privados, la Cámara de Comercio Internacional y la Organización para la Cooperación y el Desarrollo Económico (OCDE).

Toda la información sobre esta Conferencia puede encontrarse en el siguiente hipervínculo:

<http://www.privacyconference2006.co.uk/>

En marzo del año 2006 tuvo lugar el I Congreso Europeo de Protección de Datos, organizado por la Agencia Española de Protección de Datos, en colaboración con la Fundación BBVA y el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

El Congreso consiguió reunir por primera vez en un mismo foro a los máximos representantes de las Autoridades Europeas de Protección de Datos, expertos en la materia y cualificados representantes del ámbito político y empresarial no sólo de Europa, sino también de EE.UU. e Iberoamérica, y surgió con el objetivo de crear un foro abierto para permitir la puesta en común del conocimiento y el esfuerzo de todos los agentes implicados en la salvaguardia del derecho fundamental a la protección de datos, tanto del sector público como del sector privado.

En el Congreso, que se dividió en torno a 6 paneles, se tuvo la oportunidad de tratar temas como el desarrollo reglamentario de la Ley Orgánica de Protección de Datos debatiéndose las principales novedades del texto que entonces ya estaba siendo elaborado.

Se analizó igualmente la Directiva europea sobre protección de datos exponiéndose el trabajo desarrollado por el Grupo de Trabajo del Artículo 29 y analizando el marco jurídico de la protección de datos más allá de nuestras fronteras.

También fueron objeto de análisis las transferencias internacionales de datos basadas en las llamadas Binding Corporate Rules o Reglas Vinculantes de las Corporaciones y su aplicación en la actividad económica en el sector privado.

Asimismo, se trató la relación entre la lucha contra el fraude y la protección de datos, destacando las propuestas europeas de la lucha contra el fraude en el sector financiero y su incidencia en la privacidad y por tanto en la protección de datos personales.

Del mismo modo, se analizó la lucha contra el terrorismo y la delincuencia organizada y su conexión con la protección de datos, examinando los instrumentos jurídicos para la lucha contra el terrorismo y la delincuencia y las novedades introducidas por la normativa de retención de datos de tráfico.

Por último, se debatió sobre la tensión entre la transparencia en las actividades públicas, la protección de datos y el rápido desarrollo de las nuevas tecnologías de la información.

COOPERACIÓN EN LA LUCHA CONTRA EL SPAM: CONTACT NETWORK OF SPAM AUTHORITIES Y LONDON ACTION PLAN

El "London Action Plan" es un foro de debate que reúne a organizaciones tanto públicas como privadas de 27 países, responsables del cumplimiento de las leyes que luchan contra el Spam. Entre ellas se encuentra una amplia representación de agencias de protección de datos, agencias de telecomunicaciones y de protección de los derechos de los consumidores. Su objetivo es una cooperación para luchar contra el spam a nivel internacional, para tratar problemas tales como el fraude on-line, los engaños, el "Phising" y la difusión de virus.

Asimismo, se colabora también con otras organizaciones internacionales, tales como la Organización para la Cooperación Económica y el Desarrollo (OECD), la Unión Internacional de Telecomunicaciones (ITU), la Unión Europea (UE), la Red Internacional para el cumplimiento de las leyes de Protección al Consumidor (ICPEN), y la Cooperación Económica Asia-Pacífico (APEC).

La AEPD firmó el acuerdo del London Action Plan en octubre de 2004 y es miembro de este grupo de trabajo a nivel mundial con vistas a la colaboración en la lucha contra el Spam. Durante el año 2006 se realizaron trabajos de estudio en temas concretos, como la pornografía infantil en Internet y el futuro de la base de datos de WHOIS, que identifica la gestión de las páginas de Internet y ayuda a la persecución del fraude, a nivel mundial.

CASE HANDLING WORKSHOP

Este Grupo de Trabajo -denominado de tratamiento de quejas- se creó en el año 1999 en Helsinki en el seno de la Conferencia de Primavera de Autoridades Europeas de Protección de Datos, con el fin de dar cumplimiento a lo establecido en el Artículo 28(2) de la Directiva 95/46/CE. Su finalidad principal es comparar los procedimientos en el tratamiento de reclamaciones en las distintas autoridades de protección de datos y prestarse ayuda en procedimientos que revisten una especial sensibilidad o dificultad.

El Grupo de Trabajo de Tratamiento de Quejas se reúne semestralmente, celebrándose la decimotercera reunión en el mes de marzo en Madrid.

Los temas sobre los que giró el encuentro, entre otros, estuvieron relacionados la Administración electrónica, y la vigilancia de los trabajadores. La AEPD participó en dos sesiones con la presentación de las garantías que en materia de protección de datos supone el nuevo Documento Nacional de Identidad electrónico y con la presentación de algunos de los casos más relevantes que en materia de videovigilancia en el entorno laboral se han llevado.

La decimocuarta reunión, se celebró en Atenas, centrándose el intercambio de ideas sobre la videovigilancia, así como en sesiones paralelas en las que se compartieron experiencias respecto a los datos bancarios y financieros en las transferencia de los datos personales de los clientes de los bancos a otras instituciones financieras en caso de transacciones o contratos incompletos o la recogida y almacenamiento de este tipo de datos. Por otro lado, también se tuvo la oportunidad de compartir opiniones y prácticas en las competencias para aplicar las leyes de protección de datos y en las relaciones de las autoridades de protección de datos con los medios de comunicación.

GRUPO DE TRABAJO INTERNACIONAL DE PROTECCIÓN DE DATOS EN TELECOMUNICACIONES (IWGPDPT)

El Grupo de Trabajo Internacional de Protección de Datos en Telecomunicaciones, creado por la Autoridad de Protección de Datos y de Acceso a la Información Pública de Berlín, celebró durante el año 2006 sus reuniones número 39 y 40, en Washington y Berlín respectivamente. La AEPD participa en este grupo desde sus inicios.

En su primera reunión del año 2006 este Grupo de trabajo se centró en contenidos como la informática de confianza, los problemas relativos al fenómeno del marketing transfronterizo, con las cada vez más débiles fronteras de los países frente a la invasión de publicidad no deseada, así como la gestión segura de la información que se aloja en servidores.

Finalmente se presentaron aplicaciones prácticas de tecnologías de RFID, y las nanotecnologías.

Se adoptó un documento de trabajo sobre la disponibilidad de las historias clínicas electrónicas (Working Paper on Online Availability of Electronic Health Records cuyo texto puede ser consultado en:

(http://www.datenschutz-berlin.de/doc/int/iwgdpt/WP_HealthRecords_en.pdf)

En su segunda reunión se trataron temas relativos a los problemas derivados del uso de servicios web, identificadores por radiofrecuencia (RFID) y las tecnologías de análisis de voz. Se procedió a la aprobación de los siguientes documentos:

- Working Paper on Trusted Computing, Associated Digital Rights Management Technologies, and Privacy - Some issues for governments and software developers
- Working Paper on Privacy and Security in Internet Telephony (VoIP)

La actividad del Gabinete Jurídico se ha centrado en 2006 en el asesoramiento verbal y escrito al Director y las distintas Subdirecciones de la Agencia Española de Protección de Datos, así como en el asesoramiento a otras Administraciones Públicas, empresas y entidades dentro de las funciones que a la Agencia de Protección de Datos encomienda el artículo 37 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

Al propio tiempo, se evacuaron un total de 553 informes, resolviendo cuestiones de especial complejidad planteadas por responsables de ficheros, de los cuales 254 se refirieron a consultas planteadas por distintos Órganos de las Administraciones Públicas y 299 correspondieron a consultas formuladas por responsables de ficheros procedentes del sector privado.

Asimismo fueron informadas 73 disposiciones de carácter general, sometidas a informe preceptivo de la Agencia de Protección de Datos de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica Ley Orgánica 15/1999 y 5 b) del Estatuto Orgánico de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo.

Por otra parte, se ha participado en más de 150 reuniones de trabajo, tanto con representantes de las Administraciones Públicas como del sector privado (tanto a través de las distintas asociaciones empresariales como con empresas), celebradas con la finalidad de resolver cuestiones concretas relacionadas con la protección de datos, participando además en los distintos grupos de trabajo creados con la finalidad de resolver las cuestiones que afectan en especial a un determinado sector en la aplicación de las normas de protección de datos.

Como se ha indicado, junto con esta actividad consultiva externa se han desarrollado las funciones propias de asesoría jurídica interna de los distintos órganos de la Agencia, en las más diversas materias.

Asimismo se ha participado activamente en distintas actuaciones divulgativas de la legislación reguladora del derecho fundamental a la protección de datos, habiéndose impartido más de 40 conferencias o presentaciones sobre esta materia, tanto en foros nacionales (del sector público y privado) como internacionales.

INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

De conformidad con lo establecido en el artículo 37 h) de la LOPD corresponde a la Agencia Española de Protección de Datos informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica. Por su parte, el artículo

5 del Estatuto de la Agencia concreta, en sus apartados a) y b), este precepto estableciendo que la Agencia informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica así como cualesquiera proyectos de ley o reglamentos que incidan en la materia propia de la Ley Orgánica.

A lo largo de 2006 se han sometido al parecer de la Agencia de Protección de Datos, para su informe preceptivo, un total de 73 disposiciones, lo que supone en la práctica el mantenimiento de las cifras correspondientes al año 2005, en que se informaron un total de 76 disposiciones:

De entre las disposiciones informadas, cabe hacer referencia a las siguientes:

- Anteproyecto de Ley de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Anteproyecto de Ley de bases de datos policiales sobre identificadores obtenidos a partir del ADN.
- Anteproyecto de Ley de Administración Electrónica.
- Anteproyecto de Ley de investigación biomédica.
- Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Anteproyecto de Ley contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
- Anteproyecto de Ley de Defensa de la Competencia.
- Proyecto de Real Decreto por el que se implanta en la Administración de Justicia el sistema informático de telecomunicaciones LexNet, para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.
- Proyecto de Real Decreto por el que se suprime la exigencia de aportación de fotocopia del Documento Nacional de Identidad en los procedimientos de la Administración General del Estado.
- Proyecto de Real Decreto por el que se suprime la exigencia de adjuntar el volante de empadronamiento en los procedimientos de la Administración General del Estado
- Proyecto de Orden por la que se establece la configuración, características, requisitos y procedimiento de acceso al sistema de verificación de datos de identidad.
- Proyecto de Orden por la que se establece la configuración, características, requisitos y procedimiento de acceso al sistema de verificación de datos de residencia.

- Proyecto de Real Decreto por el que se aprueba el Reglamento de exención de determinadas categorías de acuerdos de intercambio de información sobre morosidad
- Proyecto de Real Decreto por el que se regula el sistema común de presentación electrónica de documentos dirigidos a la Administración General del Estado.
- Proyecto de Real Decreto por el que se desarrolla la Ley 20/2005, de 14 de noviembre, sobre la creación del Registro de Contratos de Seguro con cobertura de fallecimiento.
- Proyecto de Real Decreto por el que se regula la publicidad de los Protocolos Familiares
- Proyecto de Real Decreto por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el Procedimiento para su actualización.
- Proyecto de Real Decreto por el que se aprueba el Reglamento general de Mutualismo Judicial.
- Proyecto de Real Decreto de desarrollo de la Ley 5/2006, de 10 de abril, de Regulación de los Conflictos de Intereses de los Miembros del Gobierno y de los Altos Cargos de la Administración General del Estado.
- Proyecto de Real Decreto regulador de la trazabilidad de los medicamentos de uso humano.
- Proyecto de Real Decreto por el que se modifica el Real Decreto 1199/1999, de 9 de julio, por el que se desarrolla la Ley 13/1998, de 4 de mayo, de Ordenación del mercado de tabacos y normativa tributaria, y se regula el estatuto concesional de la red de expendedurías de tabaco y timbre.
- Proyecto de Real Decreto por el que se establecen normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de las células y tejidos humanos y se regulan las normas de coordinación y funcionamiento para su uso en humanos
- Proyecto de Orden Ministerial por el que se establecen los requisitos de trazabilidad y la notificación de reacciones y efectos adversos graves de la sangre y de los componentes sanguíneos.
- Proyecto de Decreto Foral por el que se establece el régimen general de seguridad de los sistemas de información y de las comunicaciones en la Administración de la Comunidad Foral de Navarra.
- Proyecto de Orden por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas.

- Proyecto de Orden por la que se modifica la Orden de 25 de abril de 1994 por la que se regulan las recetas y los requisitos de prescripción y dispensación de estupefacientes para uso humano.
- Proyecto de Orden por la que se aprueba la Declaración de Prácticas y Políticas de Certificación del Documento Nacional de Identidad Electrónico.

Además, debe indicarse que entre los proyectos de disposiciones generales informadas en el periodo comentado, ha sido especialmente significativo el número de disposiciones dirigidas a la creación de ficheros o a la modificación de disposiciones ya existentes que los regulaban, muy particularmente en el ámbito de la Administración General del Estado.

Así, durante el período analizado, han sido sometidas a informe disposiciones de creación o modificación de ficheros de los Ministerios de Fomento, Medio Ambiente, Educación y Ciencia, Defensa, Economía y Hacienda, Interior, Agricultura, Pesca y Alimentación y Presidencia. Asimismo, han sido informados los Acuerdos de creación de ficheros del Consejo General del Poder Judicial y los Órganos Jurisdiccionales, así como de distintos Colegios profesionales y Consejos Generales.

Igualmente, debe reseñarse que en la última quincena de 2006 ha sido sometido a informe de la Agencia el Proyecto de Reglamento de desarrollo de la LOPD, habiéndose emitido informe en fecha 17 de enero de 2007, de cuyo contenido se dará cuenta en la Memoria correspondiente a dicho ejercicio.

INFORMES SOBRE CONSULTAS PLANTEADAS POR RESPONSABLES DE FICHEROS

INTRODUCCIÓN

Como se ha indicado, el Gabinete Jurídico ha venido ejerciendo, desde la creación de la Agencia Española de Protección de Datos, una función de asesoramiento externo, emitiendo dictámenes jurídicos sobre las cuestiones de mayor complejidad sometidas al parecer de la Agencia por los responsables de ficheros, tanto particulares como Administraciones Públicas.

Durante el año 2006 se ha mantenido el importante volumen de actividad desplegado en el ejercicio de esta función. Así, en el periodo de referencia, han sido emitidos un total de 553 informes, lo que supone un ligero descenso, inferior a un 5%, respecto de los rendidos durante el año 2005, siendo el incremento acumulado sobre el año 2002 de en torno a un 40%. Por otra parte, debe destacarse cómo en los últimos años se ha incrementado notablemente, en muchos casos, la complejidad de las cuestiones

planteadas, descendiendo correlativamente el volumen de consultas que han sometido cuestiones de mayor simplicidad o reiteradas otros años.

De este modo, cuestiones planteadas de modo reiterado en años anteriores han ido descendiendo en estos últimos años en gran número, habida cuenta de la importante labor divulgativa efectuada durante esos ejercicios anteriores, que ha permitido conocer en profundidad dichas materias, reduciendo el número de consultas relacionadas con las mismas. A título de ejemplo, las cuestiones relacionadas con el tratamiento y cesión de los datos del padrón municipal han descendido ininterrumpidamente desde las casi 100 planteadas en 1999 a las 24 formuladas en 2006. Del mismo modo, se ha reducido ampliamente el volumen de consultas relativas al tratamiento de datos por las entidades dedicadas a la prestación de servicios de solvencia patrimonial y crédito o las referidas a la aplicación del Reglamento de Medidas de Seguridad, sin perjuicio de que es previsible un incremento futuro de las mismas en caso de aprobación del Reglamento de desarrollo de la Ley Orgánica 15/1999.

Por su parte, se han estabilizado las cifras referidas a las consultas relacionadas con las transferencias internacionales de datos, el tratamiento de datos por operadores de comunicaciones electrónicas, el tratamiento de datos de salud, así como el de los restantes datos especialmente protegidos, que sufrieron un elevado incremento en los años 2005 y 2006 respecto de ejercicios anteriores. Igualmente es destacable el incremento de las consultas relacionadas con el modo en que deberán ser atendidos los derechos de acceso, rectificación, cancelación y oposición, que duplican las efectuadas en el año 2005.

Por su parte, se produce una reducción de las consultas relacionadas con los ficheros el tratamiento de datos por parte de las Administraciones Tributarias, así como de las relacionadas la realización de distintas actividades de recogida y tratamiento de datos a través de Internet, que habían tenido un gran incremento en 2005, situándose sus cifras en los niveles existentes en 2004.

Del volumen de informes evacuados a instancia de responsables de ficheros durante el año 2004, 299 (un 54%) han correspondido a consultas privadas, mientras que 254 (un 46%) han sido las planteadas por las Administraciones Públicas, pudiendo reseñarse que en este año ha seguido siendo mayor (al igual que ocurrió en años anteriores) el número de consultas planteadas por particulares (personas físicas o jurídicas) manteniéndose exactamente la misma proporción que existía en el ejercicio anterior.

Considerando estas cifras, puede apreciarse cómo, respecto a las cuestiones planteadas por el sector público, la inmensa mayoría de las mismas han sido formuladas por Administraciones Públicas territoriales, estabilizándose en torno al 15% el peso de las consultas planteadas por Órganos no integrados en dichas Administraciones. Ello puede deberse a la constante difusión efectuada por esta Agencia del contenido de la normativa en materia de protección de datos en relación con estos colectivos, en particular con las Entidades que integran la denominada Administración Corporativa, en desarrollo de los protocolos de cooperación celebrados en ejercicios anteriores.

Por otra parte, se ha reducido sensiblemente el número de informes elaborados a solicitud de la Comisión del Mercado de las Telecomunicaciones, que alcanzan un número de 7, frente a los 32 del ejercicio anterior.

Al propio tiempo, se estabiliza el reparto existente entre las consultas procedentes de la Administración General del Estado (un 45% del total del sector público) y de las Administraciones autonómica y local (15% y 26%, respectivamente), con un ligero repunte de las procedentes de la Administración Local, pese a la progresiva disminución de las consultas relacionadas con el padrón municipal de habitantes, a la que ya se ha hecho referencia.

Por su parte, en cuanto a las consultas del sector privado, y al igual que ha venido sucediendo en años anteriores, predominan notablemente las consultas planteadas por empresarios (dos tercios del total).

Atendiendo a la distribución sectorial de las consultas, cabe destacar que se mantiene la reducción en términos porcentuales sobre el total de consultas planteadas de las provenientes de entidades dedicadas a actividades de asesoría y consultoría. De este modo, y como ya sucedió en el ejercicio anterior, este sector ya no es siquiera el que plantea un número superior de consultas, habiendo sido superado por los prestadores de servicios de comunicaciones electrónicas. Ello se debe, como se ha señalado en las Memorias correspondientes a ejercicios anteriores, al hecho de que las consultas planteadas se han centrado en las relativas a la gestión de los propios ficheros de estas entidades de asesoría, dado que, como se ha indicado en anteriores Memorias, se ha dejado constancia a las mismas de que, en lo referente a las cuestiones planteadas en relación con la función asesora de los clientes responsables de ficheros, se estaría obligando a la Agencia de Protección de Datos (al margen de las previsiones de la Ley Orgánica y de su Estatuto) a llevar a cabo actividades propias de dichas entidades, entrando en concurrencia con éstas.

Como sucedía en relación con las materias objeto de consulta, la tendencia respecto al ejercicio anterior es el mantenimiento de las cifras y porcentajes correspondientes a los distintos sectores. De este modo, los principales incrementos se producen en sectores con un peso más reducido en esta actividad de la Agencia, tales como el sector educativo y el de la publicidad y prospección comercial (un 62% y un 33% respectivamente), siendo también de menor peso los sectores en que se producen las mayores disminuciones: el del transporte y el de las asociaciones de consumidores (con reducciones de un 41% y un 31%, respectivamente).

Por otra parte, se mantiene la cifra de las consultas formuladas por los prestadores de servicios de comunicaciones electrónicas, que mantienen el primer lugar, habiéndose incrementado en casi un 90% en estos dos últimos años. En este sentido, han de tenerse en cuenta las competencias atribuidas a la Agencia Española de Protección de Datos por el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

En particular, el artículo 109.1 del citado Reglamento dispone que "Los operadores que presten servicios de comunicaciones electrónicas remitirán los contratos a los que se hace referencia en los artículos anteriores y sus modificaciones, con al menos 10 días de antelación a su entrada en vigor, al Ministerio de Industria, Turismo y Comercio, a la Comisión del Mercado de las Telecomunicaciones, al Instituto Nacional del Consumo, a la Agencia Española de Protección de Datos y al Consejo de Consumidores y Usuarios. Este último organismo la pondrá a disposición de las asociaciones de consumidores y usuarios integradas en él".

Asimismo, según dispone el artículo 71.2, "los operadores que vayan a prestar las facilidades de identificación de la línea de origen o de la línea conectada deberán remitir al Ministerio de Industria, Turismo y Comercio y a la Agencia Española de Protección de Datos, con carácter previo a la prestación de estas facilidades, un documento que recoja las características y los procedimientos empleados para garantizar el cumplimiento de lo establecido en este Reglamento sobre dichas facilidades".

Así, en el año 2006 se emitieron 32 informes preceptivos derivadas de la aplicación del mencionado precepto, frente a los 41 emitidos en 2005.

Debe igualmente destacarse el mantenimiento de las cifras del ejercicio anterior en los sectores sanitario y farmacéutico, que se había incrementado un 50% en el ejercicio 2005, así como en relación con las consultas provenientes de asociaciones de consumidores y usuarios.

Además, se ha incrementado ligeramente el número de consultas formuladas por las asociaciones empresariales y profesionales, siendo dicha cifra seis veces superior a la registrada en 2002. Este hecho resulta relevante, dado que dichas consultas son generalmente objeto de difusión por las propias asociaciones, con el consiguiente efecto de resultar conocidas por gran parte del sector al que las mismas pertenezcan.

A diferencia de otros años, se ha producido un cierto cambio de tendencia en lo referente a la distribución geográfica de las consultas. Así, se ha producido un notable incremento de las consultas formuladas desde Andalucía (de prácticamente un 50%), que ha pasado a ocupar el segundo lugar en cuanto a las Comunidades Autónomas de procedencia, reemplazando en dicha posición a Cataluña que ha reducido ligeramente sus cifras respecto de 2005. Igualmente, es destacable el profundo descenso de las consultas procedentes de la Comunidad Valenciana, que disminuye en casi un 40%, y de Aragón, que disminuye en más de un 70%.

Por lo demás, las consultas procedentes de la Comunidad de Madrid representan más de un 45% del total, siendo relevante, a nivel provincial, el incremento producido en el número de consultas procedentes de Málaga, Sevilla, Baleares y Tarragona, frente a los muy notables descensos de Valencia y Zaragoza.

Finalmente, en lo referente a la distribución de consultas atendiendo a la materia sobre la que las mismas versan, puede observarse que predominan aquellas relativas a las cesiones de datos, siendo más relevante el número de consultas relacionadas con las

cesiones entre entidades privadas, que este año alcanzan un 37% del total, frente al 29% del año 2005.

INFORMES DE MAYOR INTERÉS EMITIDOS DURANTE EL AÑO 2006

■ CUESTIONES GENERALES RELACIONADAS CON EL ÁMBITO DE APLICACIÓN Y LAS DEFINICIONES CONTENIDAS EN LA LOPD

En el informe 364/06 se analiza si resulta de aplicación al tratamiento de datos realizado al amparo del Reglamento (CE) Nº 881/2002, del Consejo de 27 de mayo de 2002 por el que se imponen determinadas medidas restrictivas específicas dirigidas contra determinadas personas y entidades asociadas con Usamah Bin Ladin, la red Al-Qaida y los Talibanes, la excepción prevista en el artículo 2.2 c) de la LOPD, contestándose de manera negativa, al considerarse que dicha excepción únicamente podría ser aplicable a los ficheros que pudieran encontrarse amparados por el artículo 13.2 de la Directiva 95/46/CE, que en esta materia se referiría únicamente a los ficheros mantenidos en el ámbito de las Administraciones Públicas y no a los ficheros de titularidad privada que pudieran ser creados con la finalidad de transmitir a las Administraciones Públicas los datos que precisaren para el cumplimiento de las funciones descritas en el precepto. Asimismo, se aclara que el tratamiento se encontrará amparado por lo dispuesto en la Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo. Por último, se reitera la excepción en este caso del cumplimiento del deber de información y la posible denegación de los derechos de acceso, rectificación, cancelación y oposición, por aplicación de la Ley 12/2003, que ya había sido puesta de relieve en informes anteriores.

En el informe 64/06 se analiza si la administración concursal de una sociedad mercantil que no había cumplido con las obligaciones previstas en la LOPD, disponiendo de ficheros con datos de carácter personal, tanto en soporte papel, como informatizados, debe proceder al cumplimiento de dichas obligaciones, dándose respuesta afirmativa a la cuestión, a tenor de lo dispuesto en el Título II de la Ley 22/2003, de 9 de julio, Concursal, del que se deriva que corresponderá a los administradores concursales, bajo la supervisión del Juzgado competente, decidir sobre el objeto, contenido y uso del tratamiento de los datos de carácter personal de la entidad concursada. Además, se planteaba la posible enajenación de los equipos de la empresa concursada, informándose que conforme al artículo 4.5 LOPD deberá procederse previamente al borrado físico de todos los datos de carácter personal contenidos en dichos equipos.

Por su parte, en el informe 285/06 se resuelve la consulta relacionada con el sometimiento a la LOPD de la prestación de un servicio telefónico de atención a los usuarios de un servicio de taxi, en que se recogen los datos del número telefónico desde el que se realiza la llamada, asociándose a la dirección del titular. Se consideró que la realización de un tratamiento con los datos mencionados quedará sometida a las previsiones de la LOPD.

En cuanto al ámbito territorial de aplicación de la LOPD, el informe 137/06 se refiere al supuesto de creación por una entidad española de una base de datos de profesionales de Estados Unidos y Canadá obtenida a través de varias acciones de promoción y que se ubicará en una Intranet de una Web francesa, considerando que con independencia de que los datos sean recogidos en otro país, dado que el tratamiento se efectúa en el marco de la actividad de un establecimiento del responsable del tratamiento situado en España, el mismo se encontrará sometido a la legislación española, siguiendo el criterio de interpretación, conforme a la Directiva 95/46/CE, del artículo 2.a) de la LOPD, debiendo además darse cumplimiento al artículo 12 de la citada Ley en la relación que vincula al consultante con la entidad francesa que alojará los datos.

En cuanto al ámbito subjetivo de la LOPD, el informe 365/06 analiza la conformidad con la LOPD de la posibilidad de facilitar los datos de nombre y edad de personas fallecidas a los medios de comunicación local, a través de tabloneros informativos en los accesos a las instalaciones de un tanatorio o proceder a su publicación en un sitio web. Tras insistir en la doctrina reiteradamente mantenida por la Agencia de que el derecho fundamental a la protección de datos no resulta aplicable a las personas fallecidas, por aplicación del artículo 32 del Código Civil, se advierte acerca de las posibles consecuencias que la publicación de un número excesivo de datos puede provocar en cuanto al posible ejercicio por los sujetos legitimados de las acciones previstas en la Ley Orgánica 1/1885, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Por último, en lo que respecta al concepto de datos de carácter personal, el informe 425/06 analiza si los datos contenidos en la placa de matrícula de un vehículo tienen el carácter de datos de carácter personal, respondiéndose afirmativamente a tenor del concepto contenido en el artículo 3.07 de la LOPD y el régimen establecido en el artículo 2 a) de la Directiva 95/46/CE, así como de las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiera plazos o actividades desproporcionados. Ello se funda en que el párrafo tercero del artículo 2 del Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, establece que "el Registro de Vehículos ... será público para los interesados y terceros que tengan interés legítimo y directo, mediante simples notas informativas o certificaciones", por lo que cabe considerar que la identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados y que el tratamiento del dato de la matrícula habrá de ser considerado como tratamiento de un dato de carácter personal.

Asimismo, en el informe 119/06 se plantea la conformidad con lo dispuesto en la LOPD, de las transmisiones de datos establecidas en un contrato celebrado por un laboratorio farmacéutico con distintos almacenes mayoristas, a fin de conocer las circunstancias y el precio al que han sido vendidos finalmente los medicamentos vendidos a su vez por la consultante a los citados almacenes mayoristas, lo que implica acceder a los datos de facturación de las oficinas de farmacia, planteándose si los mismos son datos de carácter personal

La cuestión debatida había sido ya objeto de numerosas consultas a la Agencia, por lo que tras recapitular sobre el contenido de las mismas y la doctrina emanada sobre esta

materia de la Sala de lo contencioso-Administrativo de la Audiencia Nacional, se concluye que el dato de facturación de las oficinas de farmacia ha de ser considerado como dato referido a la facturación de un establecimiento mercantil.

No obstante, ahondándose en el contenido de la consulta, la solicitud del dato de facturación no exige necesariamente la identificación del empresario individual titular del establecimiento mercantil en que desarrolla el comercio, lo que resulta sumamente relevante en el caso de las oficinas de farmacia, dado que el farmacéutico habrá de ejercer su actividad de dispensación así como las restantes actividades profesionales previstas en la Ley 16/1997, precisamente, a través del establecimiento mercantil en que se constituye la oficina de farmacia y dicho establecimiento por imperativo del artículo 103.4 de la Ley 14/1986, de 25 de abril, General de Sanidad deberá tener por titular o propietario, precisamente, a un farmacéutico.

De este modo, será posible la comunicación de los datos identificativos del farmacéutico en los supuestos en que el mismo haya decidido, como política empresarial, utilizar aquellos datos para identificar la sociedad que gestione el establecimiento o para determinar el rótulo del mismo, dado que en dichos supuestos no se estará cediendo más que los datos identificativos de una persona jurídica o de un establecimiento mercantil. En los demás supuestos será necesario que los datos de facturación no aparezcan vinculados al titular del establecimiento, identificándose mediante algún otro criterio, como la localización de aquél.

Por último, en cuanto a la naturaleza pública o privada de determinados ficheros, debe hacerse referencia tres informes. En el primero de ellos (informe 504/06) se hace referencia a los ficheros de las cofradías de pescadores, considerando que, dado que las actividades de las mismas, que se describen en el artículo 46 de la Ley 3/2001, de 26 de marzo, de Pesca Marítima, no implicaran en modo alguno el ejercicio de potestades administrativas ni de ninguna de las "competencias" a las que se refiere el artículo 21 de la Ley Orgánica 15/1999, sus ficheros deberán en todo caso ser considerados como de titularidad privada.

Por su parte, el informe 191/06 considera ficheros de titularidad privada los mantenidos por una Sociedad Municipal de Rehabilitación Urbana, teniendo en cuenta que la misma es una entidad de naturaleza mercantil, participada íntegramente por una Entidad Local, si bien en cuanto sus ficheros puedan referirse a la gestión de servicios municipales por la propia sociedad, la misma tendría la condición de encargada del tratamiento, siendo responsable de dichos ficheros la propia Corporación Municipal, por lo que los mismos sí serían de titularidad pública.

Similar conclusión se alcanza en el informe 287/06, en que se analizan los distintos supuestos en los que se encomienda a una entidad la gestión integral de los servicios relacionados con el suministro de agua, considerándose que dicha entidad será encargada del tratamiento, ostentando el Ayuntamiento la condición de responsable del fichero, con independencia de que el servicio sea prestado por una entidad privada, una empresa mixta (sociedad anónima o sociedad limitada), participada por capital del propio Ayuntamiento o una empresa mixta participada por un Consorcio de distintos Ayuntamientos.

■ CUESTIONES RELACIONADAS CON LA DELIMITACIÓN DEL RESPONSABLE DEL FICHERO Y DEL ENCARGADO DEL TRATAMIENTO.

El informe 46/06 reitera el criterio mantenido por la Agencia en relación con la condición de responsable del fichero de los administradores o gestores de fincas que gestionan alquileres u otras rentas inmobiliarias de los titulares de viviendas en lo que se denomina régimen de "propiedad vertical".

Por otra parte, el informe 253/06, se refiere a un supuesto en que una entidad dedicada a la prestación de servicios sanitarios se encuentra formada por dos socios, que se dedican a distintas especialidades médicas, manteniendo consultas privadas separadas, sin que los datos de los pacientes de cada uno de ellos sean accesibles por el otro, planteándose quién es el responsable del fichero. En este caso se considera que actuando los dos socios como personal de la sociedad, será ésta la responsable del fichero, sin perjuicio del necesario cumplimiento, en cuanto al acceso a las historias clínicas de lo dispuesto en la Ley 41/2002, de 14 de noviembre.

En otro orden de cosas, el informe 172/06 analiza si las empresas de trabajo temporal han de ser consideradas encargadas del tratamiento de las empresas usuarias con las que celebren en su caso un contrato de puesta a disposición de los trabajadores contratados por aquéllas, teniendo en cuenta que como consecuencia de dicho contrato el trabajador pasa a quedar sujeto a la organización y dependencia de la empresa usuaria, por lo que no existiría en la práctica acceso alguno por parte de la empresa de trabajo temporal a los datos a los que pudiese efectivamente acceder el trabajador al que se refiera el contrato, a la vista de lo dispuesto en diversos preceptos de la Ley 14/1994, de 1 de junio y del Real Decreto 4/1995, de 13 enero, que la desarrolla, se concluye que la empresa de trabajo temporal no tendrá más que una función de mediación entre el trabajador y la empresa usuaria, de modo que el trabajador pasa a someterse a las condiciones derivadas del puesto de trabajo que ocupa en la empresa usuaria, convirtiéndose en trabajador indefinido de la misma si no cesase en su prestación al término del contrato, de modo que la empresa de trabajo temporal no tendrá siquiera conocimiento de los datos a los que acceda o a cuyo tratamiento proceda el trabajador, no pudiendo adquirir los compromisos derivados del artículo 12 de la Ley Orgánica 15/1999.

Por otra parte, han sido diversos los informes relacionados con supuestos en que se ha planteado si una determinada entidad ostenta la condición de responsable o encargado del tratamiento.

Así, el informe 34/06 se refiere al supuesto en que una entidad viene realizando desde 1996 una determinada estadística, recogida expresamente en el Plan Estadístico Nacional, para cuya realización contrata los servicios de una tercera entidad con la que celebra el correspondiente contrato administrativo. Habiéndose acordado la contratación de una nueva entidad para el siguiente estudio, se solicita por el Organismo a la anterior adjudicataria la devolución de la información derivada de la prestación de su servicio y, en consecuencia, los ficheros derivados de su actividad, a lo que la aquélla se había opuesto, indicando, según se señala, que ésta es responsable del fichero y no puede proceder a ceder los datos a la consultante.

En el informe se señala que la entidad adjudicataria tiene la condición de encargada del tratamiento y el Organismo la de responsable del fichero, a la vista de los pliegos de cláusulas administrativas y prescripciones técnicas del contrato, siendo de aplicación el artículo 12.3 de la LOPD, según el cual "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". Asimismo, se recuerda que la Agencia ha venido indicando que dicha obligación podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta.

Deben igualmente recordarse los informes 191/06 y 287/06, citados anteriormente, así como el informe 303/06, en que se considera encargado del tratamiento a una empresa concesionaria en régimen de gestión directa de un determinado servicio público, teniendo en cuenta lo dispuesto en el artículo 155.2 del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, que establece que "Antes de proceder a la contratación de un servicio público, deberá haberse determinado su régimen jurídico básico que atribuya las competencias administrativas, que determine el alcance de las prestaciones a favor de los administrados y que declare expresamente que la actividad de que se trate queda asumida por la Administración respectiva como propia de la misma".

Por último, ha de hacerse por último referencia a dos supuestos específicos objeto de informe: En primer lugar, el informe 8/06 se refiere al funcionamiento del sistema que garantiza el derecho de los abonados a la conservación de su numeración en caso de cambio de operador, conocido como portabilidad numérica, que deberá ser soportado, como consecuencia de la aprobación, mediante Resolución de la Comisión del Mercado de las Telecomunicaciones de 16 de julio de 2004, de la Circular 2/2004, de 15 de julio, mediante la creación de una asociación sin ánimo de lucro que canalizaría las relaciones existentes entre los operadores como consecuencia de la necesidad de garantizar el derecho a la portabilidad numérica, prestando servicios de carácter técnico e informático que resultasen necesarios para llevar a cabo las transacciones vinculadas a la citada portabilidad. Se concluyó que la citada asociación tendría la condición de encargada del tratamiento respecto de los restantes operadores, pudiendo subcontratar la prestación del servicio, siempre que se cumplan los requisitos que la Agencia viene exigiendo para dicha subcontratación.

Por otra parte, el informe 442/06 se refiere a los ficheros gestionados por el Servicio Público de Empleo Estatal Instituto de Empleo, teniendo en cuenta que los mismos se encuentran en un gran número de supuestos relacionados con el ejercicio de competencias transferidas a las Comunidades Autónomas, a las que corresponde, según los Reales Decretos de transferencia, y en terminología no suficientemente ajustada a la LOPD, la "propiedad" de las bases de datos referidas a los afectados sometidos al ámbito de sus competencias. Teniendo en cuenta lo dispuesto en la Ley 56/2003, de 16 de diciembre, de Empleo y la doctrina reiterada de la Agencia de que en el ámbito de las

Administraciones Públicas la delimitación del responsable del tratamiento aparecerá íntimamente vinculada a la titularidad de la competencia que justifica el tratamiento de los datos de carácter personal, se considera que el Instituto será encargado del tratamiento en lo que se refiere a los ficheros comunes creados para la gestión de competencias transferidas, siendo responsable de los ficheros relacionados con las que no hayan sido objeto de transferencia. En todo caso, se recuerda la posibilidad de que el Instituto centralice el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los afectados si así se acuerda en el oportuno Convenio, bien bilateral, bien adoptado en el seno de la Conferencia Sectorial a la que se refiere la propia Ley 56/2003.

■ CUESTIONES RELACIONADAS CON LOS PRINCIPIOS DE CALIDAD DE DATOS

El informe 368/06 se refiere a la conformidad con la LOPD de la creación de un sistema de control para gestionar las ausencias y retrasos de los alumnos de un centro escolar mediante la obtención de su huella dactilar, por la que se controlaría la entrada y salida de los alumnos de dicho centro. A tal efecto, se considera que el tratamiento del dato biométrico de la huella digital para las finalidades señaladas puede resultar contrario al principio de proporcionalidad en el tratamiento, consagrado por el artículo 4.1 de la LOPD, teniendo en cuenta los precedentes contenidos en el Documento de Trabajo sobre biometría, aprobado por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, de fecha 1 agosto de 2003, referentes a decisiones adoptadas en este sentido por las autoridades de protección de datos de Francia y Portugal. Por el contrario, el informe 266/06 se refiere al supuesto de inclusión de la fotografía de los afectados en las tarjetas identificativas que los mismos deben portar en el centro de trabajo, señalándose que dicha inclusión se efectúa a fin de garantizar la identificabilidad de los trabajadores a efectos de seguridad, a fin de evitar una usurpación de los mismos por terceras personas, asegurándose así la integridad de las instalaciones. De este modo, se considera que en este caso el tratamiento sí resulta conforme al principio de proporcionalidad.

También en relación con el principio de proporcionalidad, el informe 468/06 considera excedido dicho principio en el supuesto de creación de un sistema en cuya virtud serían captadas imágenes de personas físicas a fin de analizar sus hábitos de consumo, mediante el tratamiento posterior de las imágenes relativas a su entrada o salida de un determinado local comercial, teniendo en cuenta la doctrina emanada de la Sentencia del Tribunal Constitucional 207/1996. Asimismo, se consideró que la conservación de las imágenes durante un período de dos años excedería igualmente el principio de conservación, consagrado en el artículo 4.5 LOPD.

El informe 180/06 analiza un supuesto específico relacionado con la creación de un sistema en que una empresa prestaría servicios a los contratistas y subcontratistas consistente en el acceso por aquéllos a los datos referidos al cumplimiento por parte de éstos de sus obligaciones en materia de seguridad social. Para ello, la empresa accedería a los datos obrantes en los ficheros de los que es responsable la Tesorería General de la Seguridad Social, referidos a los documentos TC2 presentados por las empresas subcontratistas, manteniendo dichos datos en un fichero al que daría posterior acceso a

las empresas contratistas, permitiendo así a estas conocer el efectivo cumplimiento de aquellas obligaciones. En un informe adjunto a la consulta se señalaba que la intervención de la empresa sería en nombre y por cuenta de las entidades contratistas y subcontratistas, ostentando la empresa intermediaria la condición de encargado del tratamiento.

El informe considera este sistema innecesario, y en consecuencia, contrarias a los principios de calidad de datos los accesos y cesiones previstas en el mismo, dado que, conforme a lo dispuesto en el Estatuto de los Trabajadores, las empresas contratistas quedarán exoneradas de la responsabilidad derivada del incumplimiento por parte de la entidad subcontratista de sus obligaciones en materia de seguridad social en caso de que hayan obtenido de la Tesorería General de la Seguridad Social la certificación a la que se refiere su artículo 42.1 o dicha certificación no haya sido emitida en el plazo de treinta días legalmente previsto, por lo que el tratamiento al que se refiere la consulta resulta excesivo en relación con la finalidad perseguida, que queda solventada por el procedimiento descrito en el Estatuto.

En cuanto al principio de finalidad, a los efectos previstos en el artículo 4.2 LOPD, el informe 184/06 se refiere al supuesto en que una determinada persona obtuvo del Registro de Vehículos los datos referidos al vehículo del que es titular la Vicepresidenta de una Comunidad Autónoma y los facilitó a un tercero, no identificado, para su difusión en forma de fotocopias repartidas en distintas dependencias del Parlamento Autonómico, considerando que dicha difusión suponía la utilización de los datos para un fin incompatible con el que había justificado su recogida mediante solicitud del Registro de Vehículos, dado que si la normativa reguladora del registro exige la concurrencia en el interesado de un "interés legítimo y directo" en conocer el contenido del mismo, no es posible que pueda apreciarse como justificante del acceso la divulgación de su contenido entre personas respecto de las cuales el responsable del propio Registro no podrá tener conocimiento de la concurrencia del citado interés ni acordar o desestimar un potencial acceso solicitado por las mismas.

Por último, el informe 127/06 se refiere a los plazos de conservación y, en su caso, cancelación del número de tarjeta de crédito de las personas físicas que realizan una compra a través de una tienda on-line o telefónicamente, recordándose que el artículo 16.5 LOPD prevé la conservación "durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre las persona responsable del tratamiento y el interesado", de modo que concluida la relación negocial, procede la cancelación de los datos, sin perjuicio de que la misma deberá dar lugar a su bloqueo en los términos previstos en el artículo 16.3 de la propia Ley, no pudiendo en ningún caso emplearse los datos para ninguna otra finalidad salvo que mediara el consentimiento del afectado para ello.

■ CUESTIONES RELACIONADAS CON DATOS ESPECIALMENTE PROTEGIDOS

El informe 431/06 analiza si el la inscripción en el Registro Civil de un matrimonio entre personas de un mismo sexo implica el tratamiento de datos especialmente protegidos relacionados con la vida sexual de los afectados, considerando que según el artículo 1

de la Ley del Registro Civil de 8 de junio de 1957 en el mismo se inscribirán "los hechos concernientes al estado civil de las personas". De este modo, dado que la celebración del matrimonio tiene tal consideración, siendo posible desde la entrada en vigor de la reforma del Código Civil operada por la Ley 13/2005, de 1 de julio, la celebración de matrimonio por personas del mismo sexo, y no habiéndose considerado hasta entonces que la inscripción del matrimonio de personas de distinto sexo constituía un dato relacionado con la vida sexual de los contrayentes, debe concluirse que los datos relativos al hecho del matrimonio siguen sin ser considerados datos de esa naturaleza.

En relación con los datos de salud, los informes 391/06 y 484/06 se refieren al tratamiento y comunicación de datos entre entidades que desarrollan actividades de prevención de riesgos laborales cuando se produce un cambio en el servicio de prevención y su adecuación a lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, considerándose dicha transmisión conforme a la LOPD como consecuencia de las obligaciones derivadas de los artículos 23.1 d) y 30.3 de la Ley 31/1995, así como de la obligación de mantenimiento de la historia clínico-laboral prevista en el artículo 37.3c) del Real Decreto 39/1997, si bien se prohíbe la transmisión de la información médica obtenida al amparo de lo dispuesto en la Ley de Prevención de Riesgos Laborales a cualquier tercero distinto del "personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores".

Por su parte, el informe 5/06 analiza si la recogida de datos relacionados con la salud visual de los clientes de un establecimiento de óptica ha de contar con el consentimiento del interesado o si cabe considerar el mismo realizado como consecuencia de la asistencia sanitaria prestada al cliente, recordando que el Real Decreto 1277/2003, de 10 de octubre, por el que se establecen las bases generales sobre autorización de centros, servicios y establecimientos sanitarios, que desarrolla lo previsto por los artículos 26.2 y 27.3 de la Ley 16/2003, de 28 de mayo, considera dichos establecimientos como "establecimientos sanitarios", por lo que el tratamiento de datos de los clientes se encuentra amparado por lo dispuesto por los artículos 7.6 y 8 de la LOPD.

A su vez, el informe 203/06 se refiere a la posibilidad de que un Tribunal de oposición, en el proceso de una convocatoria pública para la provisión de plazas de bombero tenga acceso a los resultados del reconocimiento médico realizado a los aspirantes, dado que la clínica contratada para la realización del reconocimiento ha comunicado a la consultante que únicamente informará sobre la condición de apto o no apto de los opositores, indicando que salvo que los aspirantes hayan consentido expresamente a que por parte de la clínica que realiza los reconocimientos, se comuniquen los resultados de los análisis practicados, la comunicación de datos planteada no resultará conforme a la LOPD.

Igualmente, el informe 12/06 se refiere a la posibilidad de que una Consejería pueda comunicar determinados datos a un determinado Ayuntamiento, dada la incidencia de dicha información a efectos fiscales, entre los que se encontrarían los referidos a la minusvalía de los afectados. Como regla general, se indica que no puede considerarse que el mero hecho de que las normas tributarias de ámbito local establezcan una determinada exención o deducción resulte suficiente para considerar sin más que

dichas previsiones habilitan la cesión de los datos, dado que será el propio afectado, beneficiario de la exención o deducción, quien deberá invocar la concurrencia en el mismo de la causa de la exención o deducción. No obstante, en caso de que los datos sean solicitados a fin de proceder a la comprobación de la concurrencia en un afectado concreto de los requisitos necesarios para la obtención de la exención o deducción planteada, podría resultar aplicable al supuesto lo dispuesto en el artículo 93.1 de la Ley General Tributaria.

El informe 18/06 se refiere a diversas cuestiones relacionadas con el tratamiento de datos de salud llevado a cabo en los distintos centros penitenciarios, así como a la inclusión de los datos contenidos en la historia clínica llevada por los servicios de salud penitenciaria en las historias clínicas centralizadas que eventualmente sean creadas por los servicios de salud de las Comunidades Autónomas, indicando que no será necesario el consentimiento del interno para que el personal sanitario penitenciario pueda consultar los datos que pudieran existir en el fichero centralizado de historias clínicas de un determinado sistema de salud autonómico (a la vista de lo dispuesto en los citados artículos 7.6 y 8 de la Ley Orgánica 15/1999 y en el artículo 16.1 de la Ley 41/2002) ni para el tratamiento de los datos por parte del personal sanitario penitenciario y su inclusión en el fichero centralizado de historias clínicas (por aplicación de los artículos 61 de la Ley General de Sanidad así como de lo dispuesto en la Ley 41/2002 y en la disposición adicional sexta de la Ley 16/2003), si bien deberá evitarse la inclusión de cualquier dato que permita dar a conocer el hecho de que el tratamiento ha sido prestado por un servicio sanitario penitenciario.

El informe 57/06 se refiere a la procedencia de exigir en la convocatoria anual de subvenciones para la concesión de ayudas destinadas a asociaciones, fundaciones, entidades e instituciones sin ánimo de lucro, cuyo objeto sea la atención a las víctimas del terrorismo, la aportación, contenida en la convocatoria referida al último ejercicio, de una relación nominal de víctimas, con indicación de si se trata de víctimas directas o familiares y, en este caso, su grado de parentesco con la víctima, considerando que sería más acorde a lo dispuesto en la LOPD reemplazar la exigencia de este requisito por la certificación por los órganos representativos de la entidad solicitante del número de víctimas pertenecientes a la misma, con indicación de las que son víctimas directas o familiares y el grado de parentesco de éstos con la víctima, pero sin la inclusión de una relación nominal de las mismas.

El informe 453/06, reiterado por otros de la misma naturaleza, analiza si la cumplimentación de un parte de lesiones por violencia de géneros o malos tratos, que han de efectuar los médicos y trasladar a la Autoridad Judicial, infringe la LOPD, considerándose la cesión de los datos amparada por los artículos 259 y 262 de la Ley de Enjuiciamiento Criminal.

■ CUESTIONES RELACIONADAS CON CESIONES DE DATOS

En primer lugar, cabe hacer referencia a dos supuestos de cooperación bilateral que implican cesiones de datos, contenidos en los informes 247/06 y 318/06. El primero de ellos se refiere a la celebración de un Acuerdo entre el Gobierno del Reino de España y

el Gobierno de la República Francesa a cuyo tenor se producirá un intercambio de información entre las autoridades de ambos Estados sobre los titulares del certificado de matriculación de vehículos contenidos en los ficheros nacionales de matriculación de vehículos con el fin de sancionar las infracciones contra las normas de circulación, considerándose que la cesión derivada del Acuerdo encuentra cobertura en el artículo 39.1 del Convenio de Aplicación de Schengen, así como en los artículos 12 y 27.1 del Tratado de Prüm relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, ratificado por el Reino de España el 17 de febrero de 2006.

El informe 318/06 se refiere a la procedencia o no de adoptar por parte del Consejo Superior de Deportes medidas de cooperación internacional con Francia encaminadas a la erradicación del dopaje en el deporte, consistentes en remitirles la información relativa a posibles infracciones a la disciplina deportiva en esta materia. El informe fue emitido antes de la aprobación de la Ley Orgánica de Protección de la Salud y de Lucha contra el Dopaje en el Deporte. Dicho lo anterior, la cesión se consideró conforme a la LOPD, teniendo en cuenta lo dispuesto en el Convenio nº 135 del Consejo de Europa, de 16 de noviembre de 1989, contra el dopaje, ratificado por España por instrumento de 29 de abril de 1992, que impone a las partes el deber de cooperar estrechamente en los ámbitos a que se refiere el presente Convenio, fomentando una cooperación análoga entre sus organizaciones deportivas, imponiendo el artículo 8.5, en relación con el 4.1, una cooperación estrecha bilateral y multilateral para reducir la disponibilidad (y, en particular, disposiciones encaminadas a controlar la circulación, la tenencia, la importación, la distribución y la venta) así como la utilización en el deporte de agentes de dopaje y de métodos de dopaje prohibidos y, en particular, de esteroides anabolizantes.

Por otra parte, han sido reiteradas las consultas relacionadas con la aplicación de los artículos 10 y 11 del Reglamento de Información al Consumidor en la compraventa y Arrendamiento de viviendas en Andalucía, promulgado por Decreto 218/2005 de 11 de octubre del Consejo de Gobernación de la Junta de Andalucía, según el cual se prevé el tratamiento y cesión por los intermediarios de los datos del propietario, las cargas registrales de las fincas que vayan a ser objeto de oferta, así como de las servidumbres, y certificaciones tributarias de encontrarse el transmitente al corriente del pago del Impuesto sobre Bienes Inmuebles.

El informe 44/06, a título de ejemplo, analiza la cuestión, considerando que el tratamiento y la cesión de los datos que procedan tanto del Registro de la Propiedad como del Registro Mercantil, se encuentran amparados en las normas que otorgan publicidad a estos Registros, no siendo sin embargo dicha norma aplicable a los supuestos de cesión de los datos contenidos en certificaciones tributarias, al ser preciso tener en cuenta el criterio más restrictivo, consagrado por el artículo 95 de la Ley General Tributaria, que no prevé ningún supuesto que legitime al intermediario a obtener directamente las certificaciones tributarias, lo que en consecuencia exige que se otorguen directamente al propio contribuyente y que éste las facilite al intermediario, encargado de la gestión, de forma que para que éste pueda tratar dichos datos requerirá en todo caso el consentimiento del afectado.

En relación con el Padrón Municipal de habitantes, el informe 87/06 considera conforme a la LOPD la utilización por el alcalde de los datos del citado fichero con la finalidad de remitir una carta de bienvenida a los nuevos vecinos, teniendo en cuenta la doctrina derivada de la Sentencia de la Audiencia Nacional de 21 de abril de 2004.

Por otra parte, el informe 470/06 analiza detalladamente los distintos supuestos de comunicación de los datos contenidos en los ficheros municipales a los concejales de la oposición en un determinado Ayuntamiento, diferenciando los criterios generales, los derivados para el padrón municipal de la Ley de Bases de Régimen Local y los aplicables a los ficheros de naturaleza tributaria.

En el ámbito de la Administración Pública, el informe 16/06 resuelve la consulta consistente en determinar si un Órgano de la Administración Pública puede facilitar a un funcionario que ha participado en un concurso específico de méritos para la provisión de puestos de trabajo el acceso a los datos relativos a las puntuaciones obtenidas por los participantes en dicho concurso, así como al resto de las circunstancias y datos de carácter personal que obran en el correspondiente expediente, considerando que el principio de publicidad consagrado por el artículo 19.1 de la Ley 30/1984, habilita la publicidad de la Resolución recaída en el expediente, de conformidad con lo dispuesto en el Reglamento de Ingreso del personal al servicio de la Administración General de Estado y de Provisión de puestos de trabajo y promoción profesional de los funcionarios civiles de la Administración General del Estado, de forma que, sin perjuicio del acceso que pudiera derivarse de la interposición del correspondiente recurso, la cesión queda limitada a los datos contenidos en la mencionada Resolución.

En materia sancionadora, el informe 197/06 analiza el supuesto referido a la conformidad con lo dispuesto en la LOPD del acceso por el denunciado en un expediente de infracción urbanística a los datos identificativos de la persona que le denuncia y de los funcionarios responsables en la tramitación del procedimiento. En cuanto a los datos del denunciante, se recuerda que su conocimiento no puede ser considerado como una modalidad del derecho de acceso ejercitado por el denunciado, dado que dicho derecho es definido por la Ley como el de 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, siendo así el conocimiento de dichos datos una cesión de datos. Dicho lo anterior, por aplicación de los principios y derechos contenidos en la Ley 30/1992, y en particular el de acceso permanente al expediente sancionador, se considera que, a menos que se señale expresamente en el procedimiento, tal y como sucede en el ámbito tributario, que la denuncia no forma parte del expediente administrativo, el acceso a los datos del denunciante se encontrará amparado por la LOPD. Asimismo, si el denunciante ha manifestado expresamente su deseo de confidencialidad o a juicio de la Unidad que deba resolver se entiende la necesidad de garantizar la identidad del denunciante sería posible, conforme al artículo 70.3 de la Ley de Bases del Régimen Local, denegar el acceso a estos datos. En cuanto a la identificación de las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos, el conocimiento de este dato se encuentra amparado por el artículo 35.b) de la Ley 30/1992.

También en el ámbito del derecho administrativo sancionador, el informe 550/06 analiza si resulta conforme a la LOPD la publicación de la totalidad de las sanciones impuestas en materia de disciplina deportiva por las respectivas federaciones deportivas, teniendo en cuenta las circunstancias específicas derivadas de las sanciones en esta materia y su necesario conocimiento por terceros. Tras delimitar el alcance de la aplicación de la LOPD en este caso y aclararse que la publicidad únicamente podría referirse al contenido de la resolución sancionadora, se considera que el artículo 79 de la Ley 10/1990, de 15 de octubre, del deporte establece determinadas sanciones cuya imposición implicará necesariamente el conocimiento de los datos por parte de terceros para que puedan hacerse realmente efectivas, tales como las sanciones de clausura del recinto deportivo, prohibición de acceso al estadio, pérdida de la condición de socio y celebración de la competición deportiva a puerta cerrada, amonestación pública, inhabilitación temporal de dos meses a un año, destitución del cargo, descenso de categoría o expulsión, temporal o definitiva, de la competición profesional, previstas en el citado precepto, encontrándose así la publicidad de estas sanciones habilitada por este precepto. En los restantes supuestos, la publicidad sólo será posible en caso de que se haya previsto expresamente en los estatutos reguladores de las correspondientes federaciones deportivas.

Resulta igualmente interesante el informe 233/06, que se refiere a la utilización del fichero de asociados de una Cámara Oficial de la Propiedad Urbana ubicada en el País Vasco por parte de una asociación creada con similar denominación, que procedió al cobro de las cuotas de los asociados a la Cámara Oficial, afirmando contar con el consentimiento tácito de aquéllos, en que no se describía adecuadamente la situación existente en la realidad. Las Cámaras Oficiales de la Propiedad Urbana fueron suprimidas por Real Decreto-Ley 8/1994, de 5 de agosto, previendo la disposición adicional trigésima de la Ley 66/1997, de 30 de diciembre que las Comunidades Autónomas que hayan constituido o constituyan entidades representativas del sector inmobiliario urbano con la denominación de Cámaras de la Propiedad u otras similares, adecuarán su actuación en todo caso a los principios contenidos en la presente disposición. La materia se encuentra regulada actualmente en el Decreto 15/2006, de 31 de enero, del Gobierno Vasco.

Teniendo en particular en cuenta que no existe vínculo alguno ni sucesión entre la Cámara Oficial de la Propiedad Urbana y la asociación posteriormente constituida por los integrantes de sus órganos directivos, la utilización de los datos de los asociados a la Cámara Oficial por parte de la asociación implicará la existencia de una cesión de datos de carácter personal, debiendo obtenerse el consentimiento de los afectados, que obviamente habrá de ser recabado antes de proceder a su utilización, lo que no sucedía en este caso.

El informe 526/06 se refiere a un supuesto que suscitó cierta alarma social, referido a la comunicación al Ministerio de Fomento por una determinada compañía aérea, cuya licencia puede ser objeto de suspensión cautelar, de los datos de que disponga para identificar y localizar a todos los pasajeros afectados por dicha suspensión, a fin de que por la Dirección General de Aviación Civil pueda darse cumplimiento a las obligaciones que respecto de sus pasajeros le impone el Reglamento CE 261/2004. La cesión se consideró habilitada por la Ley, dado que el mencionado Reglamento establece en el artículo 15 una serie de obligaciones de las líneas aéreas en caso de

cancelación, disponiendo su artículo 16 que cada Estado miembro designará un organismo responsable del cumplimiento del presente Reglamento en lo que concierne a los vuelos procedentes de aeropuertos situados en su territorio y a los vuelos procedentes de un país tercero y con destino a dichos aeropuertos y que cuando proceda, este organismo adoptará las medidas necesarias para garantizar el respeto de los derechos de los pasajeros, pudiendo el pasajero reclamar ante el mismo en caso de incumplimiento.

A su vez, el informe 39/06 analiza un gran número de supuestos de tratamiento y cesión de datos que habrán de efectuarse por las Cajas de Ahorros, analizando si los mismos se encuentran amparados en la LOPD y si procede o no considerar a la entidad exonerada del deber de informar. Así, en cuanto al tratamiento de los datos referidos a los posibles conflictos de intereses de los empleados y sus familiares, se considera amparado por el artículo 78 de la Ley 24/1988, que impone a las cajas el deber de respetar los códigos de conducta aprobados por el Gobierno, siendo así que el Real Decreto 629/1993, de 3 de mayo impone a estas entidades la obligación de llevar a cabo un reglamento interno en que se hagan constar como obligaciones la de recabar información de sus empleados acerca de los posibles conflictos de interés a que estén sometidos por sus relaciones familiares, su patrimonio personal o por cualquier otra causa, así como mantener actualizada dicha información.

Igualmente, en cuanto al tratamiento de determinadas operaciones de los administradores y de los miembros de las comisiones de control en el informe de buen gobierno corporativo, así como las cesiones de los datos de los mismos, se encuentran amparadas por la disposición adicional segunda de la Ley 26/2003.

Por su parte, se analiza igualmente el supuesto de publicidad de las operaciones relacionadas con partes vinculadas, teniendo en cuenta lo dispuesto en el artículo 35, párrafo cuarto de la Ley 24/1988, siendo así que esta obligación se desprende de lo dispuesto en el Reglamento 1725/2003 de la Comisión, de 29 de septiembre de 2003, por el que se adoptan determinadas Normas Internacionales de Contabilidad de conformidad con el Reglamento (CE) no 1606/2002 del Parlamento Europeo y del Consejo, que establece en su artículo 2 que el mismo "será obligatorio en todos sus elementos y directamente aplicable en cada Estado Miembro", introduciendo la Norma Internacional de Contabilidad (NIC 24), sobre información a revelar respecto a partes vinculadas, habiendo sido la redacción de dicho apartado modificada por el Reglamento 2238/2004 de la Comisión, de 29 de diciembre de 2004.

Por último, en cuanto al tratamiento y cesión de los datos de los altos cargos de las entidades, el artículo 7 de la Ley 31/1995, de 2 de agosto, impone determinados requisitos a los Consejeros Generales de las Cajas, debiendo la entidad poder conocer su concurrencia en cada caso, por lo que el tratamiento también se encuentra legalmente habilitado.

También a solicitud de la Confederación Española de Cajas de Ahorros, se analiza en el informe 72/06 la procedencia de la comunicación por una Caja a una Diputación Provincial de los domicilios efectivos de determinados deudores, incursos en procedi-

mientos de apremio para la efectividad de las deudas tributarias, considerándose que revistiendo tales datos trascendencia tributaria la cesión se encuentra amparada en el artículo 93.1 de la Ley General Tributaria.

En el ámbito educativo cabe hacer referencia al informe 37/06, relativo a la cesión de los datos referentes a los resultados de encuestas anónimas de evaluación del profesorado a los órganos encargados de velar por la calidad y el adecuado desarrollo de las enseñanzas impartidas en un Centro Universitario, siendo así que tal transmisión de datos se encuentra prevista en los Estatutos de la Universidad. El informe considera lícita la cesión, si bien limita los cesionarios a aquéllos en que resida la competencia de control del adecuado desarrollo de las actividades formativas dentro de las Facultades, Escuelas y, dentro de las mismas, Departamentos, del Centro Universitario, en virtud de la aplicación de lo dispuesto en el artículo 21.1 de la Ley Orgánica 15/1999.

En este mismo ámbito, el informe 227/06 se refiere a la comunicación de datos relativos a los alumnos de un centro escolar, señalándose, en primer lugar, que la transmisión de los datos a los propios alumnos, cuando dichos datos se refieren a los mismos, será una forma de ejercicio del derecho de acceso, que podrá ser ejercitado directamente por el menor o a través de sus representantes legales en los términos reiteradamente manifestados en informes anteriores de la Agencia. Por su parte, la cesión de los datos a los padres del menor se encontraría amparada por el artículo 154 del Código Civil, que impone a los padres el deber de procurarles a sus hijos una formación integral.

El informe 49/06 analiza la conformidad con la LOPD del acceso a los datos contenidos en el Libro de Partos de una Casa de Cuna, pertenecientes al Archivo General de una Diputación Provincial, por parte de aquellas personas que estuvieron acogidas como expósitos, a fin de poder acceder a los datos referidos a sus padres biológicos. Teniendo en cuenta lo dispuesto en el artículo 57.1 de la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español de Patrimonio Histórico Artístico, y el hecho de que la persona que pretende realizar la consulta tiene más de cincuenta años, se considera amparada por la LOPD la cesión de datos planteada.

El informe 389/06 analiza la adecuación a la LOPD de la comunicación por un centro sanitario a la Consejería de Sanidad de una Comunidad Autónoma de un certificado de colegiación de los profesionales que desarrollan su actividad en dicho centro, emitido por el correspondiente colegio profesional, así como una copia auténtica del Título Universitario correspondiente, considerándose la cesión amparada por las funciones legalmente atribuidas a la Administración solicitante por la Ley autonómica aplicable, así como por la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

En el ámbito de las relaciones laborales, el informe 252/06 se refiere a la cesión al Comité de Empresa de determinados datos relacionados con la actividad de los trabajadores de la empresa, existiendo una previsión expresa en dicho sentido en el Convenio Colectivo en vigor, considerándose que al ser dicho Convenio una de las fuentes de la relación laboral, la comunicación se encontraría amparada por el artículo 11.2 c) de la LOPD, siempre que no resulte contraria a lo dispuesto en las Leyes.

Por último, los informes 434/06 y 451/06 se refieren, respectivamente, a la publicación de los datos contenidos en las Sentencias del Tribunal Constitucional y de los datos de abogados y procuradores contenidos en los repertorios de jurisprudencia, considerándose en ambos casos conforme a la LOPD la publicidad de dichos datos, y su consiguiente cesión, aplicando a tal efecto la doctrina contenida en la Sentencia del Tribunal Constitucional 114/2006, de 5 de abril de 2006 y en la Resolución de la Agencia de 13 de enero de 2006.

■ CUESTIONES RELACIONADAS CON LOS MOVIMIENTOS INTERNACIONALES DE DATOS

Han sido reiteradas las consultas relacionadas con la posibilidad de efectuar transferencias internacionales de datos, siendo tanto el importador como el exportador de los datos entidades encargadas del tratamiento.

En los informes 518/06 y 538/06 se resume la postura de la Agencia, considerando posible la transferencia en tres supuestos concretos:

- Celebración de un contrato amparado por la Decisión 2002/16/CE entre el encargado del tratamiento, actuando en nombre y por cuenta del responsable que le hubiese otorgado poder a tal efecto, y el subcontratista.
- Celebración de un contrato entre el responsable del tratamiento y el encargado, amparado por las cláusulas previstas en la Decisión 2002/16/CE, actuando el encargado en nombre y por cuenta del subcontratista, habiéndosele otorgado poder suficiente para ello.
- Adhesión por el subcontratista a las cláusulas celebradas entre el responsable y el encargado del tratamiento, mediante un instrumento específico, firmado por las tres partes, en que el subcontratista se compromete, específicamente, al cumplimiento de las cláusulas contenidas en la Decisión 2002/16/CE (Resolución de autorización de transferencia internacional de datos de 29 de noviembre de 2006).

Por otra parte, en relación con el segundo de los supuestos citados, en el informe 196/06 se consideraba posible el establecimiento de un marco contractual formado por un único instrumento con dos partes diferenciadas: una primera referida a la prestación por el exportador de servicios al responsable del fichero en condición de encargada del tratamiento, actuando en el contrato el exportador en su propio nombre y derecho; y una segunda en que la exportadora actuará en representación de una filial de su Grupo ubicada en Chile en la que se preverá la prestación de servicios por dicha filial en condición de encargada del tratamiento para el responsable, incorporando al contrato las cláusulas establecidas en la Decisión 2002/16/CE, de la Comisión Europea, por la que se regulan las cláusulas contractuales tipo para la transferencia internacional de datos de un responsable a un encargado del tratamiento.

Por último, en el informe 538/06 ya citado, se refiere a un supuesto complejo de subcontratación en cadena, en que una entidad encargada del tratamiento subcontratará

el servicio con una tercera entidad ubicada en España, que a su vez subcontratará el servicio con otra entidad ubicada en España que, finalmente lo subcontratará con otra entidad ubicada en Chile. En el informe se considera que la transferencia internacional de datos, en los términos planteados, no se encuentra amparada por la LOPD.

■ OTRAS CUESTIONES

Debe en este punto hacerse referencia al informe 52/06, referido al Proyecto de Código Unificado de Recomendaciones sobre Buen Gobierno de las Sociedades Cotizadas, adjunto a la misma, adoptado por el Grupo Especial de Trabajo sobre Buen Gobierno creado en el seno de la Comisión Nacional del Mercado de Valores, que resulta especialmente relevante en lo relativo a la aplicación de la recomendación 67. 1 d) del Código, según la cual el Comité de auditoría deberá "establecer y supervisar un mecanismo que permita a los empleados comunicar, de forma anónima o confidencial, las irregularidades que adviertan en el seno de la empresa", teniendo en cuenta los precedentes contenidos en la Ley Sarbanes-Oxley.

El informe toma especialmente en consideración el contenido de la Opinión 1/2006 del grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE sobre la aplicación de las normas de protección de Datos de la Unión Europea a los mecanismos internos de "Whistleblowing" en el ámbito de la contabilidad y los controles internos de auditoría, la lucha contra la estafa y los delitos bancarios y financieros

Tomando todo ello en cuenta, el informe concluye que se considera por la Agencia Española de Protección de Datos necesario que dicha recomendación sea modificada en el sentido de suprimir la expresión "anónima" y que se limite el alcance de la misma a las irregularidades contables o de auditoría, reemplazando la expresión "en el seno de la empresa" por "en el ejercicio de las actividades relacionadas con la contabilidad de la empresa o la labor de los auditores".

Asimismo, se recuerda que "debería incorporarse al Código, una recomendación específica que desarrolle los mecanismos establecidos en la ya citada y que debería, cuando menos referirse a la obligación de la sociedad de informar sobre la existencia de estos mecanismos en los contratos que celebre con las personas que pudieran resultar afectadas y el cumplimiento del deber de informar al denunciado, como máximo, en los tres meses siguientes al tratamiento de sus datos de lo dispuesto en el artículo 5.1 de la Ley Orgánica 15/1999", al considerarse que el tratamiento podía entenderse amparado en los artículos 6.2 y 11.2 c) de la LOPD, en caso de ser una de las condiciones expresamente previstos en los contratos de trabajo o de servicios con las compañías que realicen actividades de auditoría. En el mismo sentido, se considera que no deberán comunicarse al denunciado los datos de quien efectúa la denuncia, al ser dicha revelación una cesión de datos no habilitada por la LOPD.

Por último, se considera necesaria la indicación de un plazo máximo de conservación de la información, el reconocimiento del derecho del interesado al ejercicio de los derechos de acceso, rectificación, cancelación y oposición y la implantación de medidas de seguridad y la notificación del fichero.

INTRODUCCIÓN

Según dispone el artículo 48.2 de la LOPD las resoluciones del Director de la Agencia de Protección de Datos ponen fin a la vía administrativa. Por ello, y sin perjuicio de la eventual interposición del recurso potestativo de reposición (al que se refiere el artículo 116 de la Ley 30/1992), dichas resoluciones sólo serán susceptibles de impugnación en vía contencioso-administrativa.

En este orden jurisdiccional, el órgano fiscalizador competente es la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Además, se han dictado algunas Sentencias por el Tribunal Supremo, que resuelven recursos de casación interpuestos contra las sentencias dictadas por los Órganos jurisdiccionales a los que se acaba de hacer referencia, en los casos en que así lo permite la Ley Rituaria.

Hasta la fecha en que se redacta la Memoria de la AEPD correspondiente a 2006, se tiene conocimiento de un total de 114 Sentencias dictadas por la Sala de la Audiencia Nacional, conociendo recursos interpuestos en primera o única instancia, y 10 Sentencias y dos Autos de inadmisión dictados por el Tribunal Supremo, resolviendo recursos de casación o casación para unificación de doctrina.

En cuanto al fallo de los pronunciamientos judiciales, debe indicarse que de las 114 sentencias dictadas en primera o única instancia, 88 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia, que quedaron plenamente confirmadas, 7 estimaron parcialmente los recursos, mientras que 18 de ellas estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia.

A la vista de estas cifras cabe apreciar un ligero descenso en el porcentaje de recursos íntegramente desestimados, que en el año 2006 representan un 77% del total de los interpuestos. Del mismo modo, el porcentaje de sentencias estimatorias dictadas por la Audiencia Nacional se ha incrementado ligeramente de un 12 a un 16 por 100 en este año.

Por su parte, el Tribunal Supremo declaró en 8 sentencias no haber lugar al recurso de casación interpuesto contra sentencias que desestimaban el recurso interpuesto contra resoluciones de la Agencia, dictando asimismo dos Autos de inadmisión del recurso también interpuesto contra sentencia desestimatoria. Asimismo, se declaró en una ocasión haber lugar a un recurso interpuesto en contra de Sentencia desestimatoria de una resolución sancionadora de la Agencia y en otra no haber lugar al recurso interpuesto por la representación de la Agencia contra la Sentencia de la Audiencia Nacional que estimó el recurso interpuesto contra la Instrucción 1/2000.

En consecuencia, con las dos únicas excepciones citadas, el Alto Tribunal vino a ratificar mayoritariamente los criterios de la Agencia en las ocasiones en que la cuestión fue sometida a su parecer.

Centrándonos en las sentencias dictadas en primera o única instancia y atendiendo al sector o ámbito de actividad al que pertenece el recurrente, puede comprobarse cómo se mantienen las cifras ya recogidas en anteriores memorias, con un amplio predominio del sector bancario. No obstante, se mantiene la reducción del volumen referido al sector de la solvencia patrimonial y crédito, incrementándose en más de un 60% el volumen de recursos promovidos por entidades pertenecientes al sector de las telecomunicaciones.

En cuanto a las materias, dentro del ámbito de la protección de datos, a las que se refería el proceso, se ha producido un ligero incremento de las relacionadas con la aplicación de los principios de calidad de datos, consolidándose como la primera de las materias a las que se refieren las sentencias, incluso por delante de las relacionadas con los ficheros de solvencia patrimonial y crédito.

En todo caso, como ya se ha indicado, al igual que en los últimos años es relevante el número de sentencias que ha guardado relación con los ficheros a los que acaba de hacerse referencia, siendo de interés examinar qué cuestiones se han tratado, en relación con los mismos, en los procedimientos judiciales finalizados en el año 2006, en las que se aprecia una mayor incidencia de las cuestiones relacionadas con la responsabilidad en caso de inclusión de datos inexactos o indebidos en los ficheros y el cumplimiento del deber de notificación de la inclusión en el fichero al deudor.

SENTENCIAS DE MAYOR RELEVANCIA DICTADAS EN PRIMERA O ÚNICA INSTANCIA

■ DELIMITACIÓN DEL CONCEPTO DE TRATAMIENTO PARA EL EJERCICIO DE ACTIVIDADES PERSONALES O DOMÉSTICAS.

La SAN de 15 de junio de 2006 estima el recurso interpuesto contra resolución de la AEPD en que se sancionaba por tratamiento de datos sin consentimiento a los miembros de la comisión organizadora de un evento, consistente en el XXV de la promoción de una Academia militar. El núcleo de la argumentación se centra en la delimitación del ámbito excluido de la aplicación de la LOPD en virtud de su artículo 2.2 a). Así, señala la Sentencia, en primer lugar que, en los supuestos en que lo personal y lo profesional aparece entremezclado, el adverbio "exclusivamente" utilizado en el art. 2.2.a) apunta a que los ficheros mixtos, en los que se comparten datos personales y profesionales, "quedarían incluidos en el ámbito de aplicación de la Ley al no tener como finalidad exclusiva el uso personal". Igualmente, se señala que "tampoco hay que entender que el tratamiento se desarrolla en un ámbito exclusivamente personal cuando es realizado por un único individuo", dado que "no deja de ser personal aquella actividad de tratamiento de datos que aún siendo desarrollada por varias personas físicas su finalidad no

trasciende de su esfera más íntima o familiar, como la elaboración de un fichero por varios miembros de una familia a los efectos de poder cursar invitaciones de boda. Y un tratamiento de datos personales realizado por un solo individuo con finalidad profesional, mercantil o industrial estará claramente incluido en el ámbito de aplicación de la Ley 15/1999". Se concluye así que "será personal (el tratamiento) cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos", de modo que en el caso analizado "la finalidad del tratamiento no excede del ámbito que acabamos de expresar pues tiene por objeto mantener los lazos de amistad y compañerismo creados durante el período formativo mediante la celebración de un acto puntual de confraternización de todos los miembros de una determinada promoción con ocasión del veinticinco aniversario de su jura de bandera", quedando así dicha actuación excluida de la aplicación de la LOPD.

■ INTERPRETACIÓN DE LOS CONCEPTOS DE FICHERO Y TRATAMIENTO

La SAN de 16 de febrero de 2006 se refiere al supuesto en que la AEPD había procedido al archivo de las actuaciones referidas a un supuesto en que la representación de un determinado sindicato en una empresa entregó a la misma un pliego de firmas de los trabajadores que había sido recabado para expresar su opinión sobre determinados aspectos de la negociación colectiva que se estaba llevando a cabo en el seno de la empresa, considerando los recurrentes que en el documento de recogida de firmas figuraban datos de los empleados, tales como nombre, código de empleado y la firma, y que la comunicación de este documento implicaba una vulneración de los artículos 7, 9 y 11 de la LOPD. La Sentencia analiza los conceptos de fichero y tratamiento, así como la delimitación del ámbito de aplicación objetivo de la Directiva 95/46/CE y la LOPD, indicando, en cuanto a éste último que "es claro para este Tribunal que registro en soporte físico equivale a fichero en los términos de la ley. Basta la lectura completa de este artículo 2 y su comparación con el art. 3 de la Directiva del que trae causa, y que sirve para interpretarlo, para llegar a esa conclusión". Por ello, "para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona". Concluye la Sentencia que "en realidad la existencia del "fichero" en el sentido legal es siempre precisa para que un tratamiento de datos personales esté sujeto al sistema de protección de la ley. En los casos de tratamiento automatizado de datos -siempre sometidos a la ley- es difícil imaginar la inexistencia de un fichero (aunque no se exija expresamente) puesto que los datos que se tratan mediante sistemas automatizados lo son siempre bajo unos criterios de estructura u organización previa".

■ DELIMITACIÓN DE LAS FIGURAS DEL RESPONSABLE DEL FICHERO Y EL RESPONSABLE DEL TRATAMIENTO

La SAN de 17 de julio de 2006 se refiere a un supuesto de tratamiento de datos referidos al conductor habitual de un vehículo de una empresa por parte de la entidad con la que la misma mantiene el vehículo en régimen de alquiler, alegándose que la cesión de los datos se fundaba en el hecho de ser el afectado el conductor habitual del mismo en el momento de realización del contrato de alquiler. A su vez los datos se comunicaron a la entidad en que el vehículo se encontraba asegurado, renovándose la póliza con fecha 24 de julio de 2002, incluyendo el dato del afectado como conductor habitual, siendo así que el mismo había sido despedido en fecha 26 de junio de 2002. La empresa, a la que se había impuesto una sanción por vulneración del artículo 4.3 LOPD aducía que no tiene en este caso la consideración de responsable del fichero ni es tampoco encargada del tratamiento, por lo que no puede estar sujeta al régimen sancionador de la Ley, dado que son las entidades titular del vehículo y aseguradora del mismo a quienes incumbe el deber de mantener los datos en sus ficheros actualizados y puestos al día. La Sentencia señala que dicha empresa "aunque no sea responsable del fichero, es responsable del tratamiento pues conjuntamente con (la titular) decidió sobre la finalidad, contenido y uso del tratamiento en los ficheros de esta última compañía de los datos personales de su empleado. Ese poder de decisión, o mejor dicho de codecisión, es precisamente el determinante de su responsabilidad".

■ NATURALEZA DEL DATO REFERIDO A LA DIRECCIÓN DE CORREO ELECTRÓNICO

La SAN de 25 de mayo de 2006 se refiere a un supuesto en que un prestador de servicios de la sociedad de la información mantenía en sus sistemas los códigos del usuario y sus respectivas claves personales de acceso de sus clientes al objeto exclusivo de dar servicio de correo a los clientes y permitir el control técnico de las comunicaciones realizadas, así como para identificar inequívocamente al cliente a los efectos de tráfico y facturación del servicio prestado, habiendo empleado los mismos para un uso incompatible con aquél y, en consecuencia, contrario al artículo 4.2 LOPD. El recurrente alegaba que la dirección de correo electrónico no constituye dato personal en los términos definidos en el artículo 3 de la LOPD, por cuanto se exige que el mencionado correo electrónico esté vinculado a la persona del titular del mismo, lo que no sucedía en este caso, dado que la dirección no identificaba en modo alguno al titular de la cuenta de correo. La Sentencia, por el contrario, señala que la Sala "considera que la dirección del correo electrónico del que es titular una persona física (...) constituye un dato personal, porque, con independencia de que la denominación de la dirección corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, lo cierto es que se puede, mediante una operación nada difícil, identificar perfectamente a una persona física, ya que esa dirección del correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio", reiterando que en su Sentencia de 27 de octubre de 2004 consideró dato de carácter personal el número del Documento Nacional de Identidad, "que en principio no tiene aparente relación externa con el nombre y apellido de su titular".

■ TRATAMIENTO DEL DATO DE LA DIRECCIÓN OBTENIDA DIRECTAMENTE DE BUZONES

La SAN de 18 de mayo de 2006 analiza el supuesto en que una determinada entidad procedió al envío de publicidad al afectado, obteniendo su dirección de la consulta personal y directa de los buzones de la zona de residencia del afectado, alegando la recurrente que los datos contenidos en el buzón deben ser considerados públicos, por lo que no es preciso contar con el consentimiento del afectado. La Sentencia señala que "el hecho de que (...) tenga su datos expuestos "al público" no puede confundirse con que dichos datos sean una fuente de acceso público pues si aparecen sus datos en el buzón es como único modo de recibir la correspondencia que pueda ser de su interés, pero dicha exposición no es confundible con una accesibilidad pública para la promoción comercial en beneficio de terceros". Por ello, debe considerarse "que los datos de los buzones que aparecen en la puerta de cada domicilio se pueden consultar para el reparto de correspondencia, pero lo que no es posible es capturar esos datos para elaborar un fichero que permita el tratamiento de dichos datos. Esto último es lo que hizo la empresa recurrente y lo que debe dar lugar a la imposición de la sanción a que se refiere la resolución recurrida".

■ TRATAMIENTO DE DATOS EN CAMPAÑAS PUBLICITARIAS

La SAN de 18 de mayo de 2006 se refiere a un supuesto de tratamiento de datos en campañas publicitarias: una determinada entidad A celebró un contrato con B, dedicada a la realización de campañas, permitiéndole el uso de los datos de sus clientes con tal finalidad. Una entidad financiera C contrató los servicios de B para la realización de una campaña, remitiéndose la publicidad a una cliente de A, que había manifestado su oposición al uso de los datos con tal finalidad. La Sentencia analiza si existe cesión en el presente caso, así como si el consentimiento de la cliente había sido válidamente obtenido, al existir una cláusula informativa en un catálogo remitido a la cliente. Respecto de la primera de las cuestiones, se alegaba que la empresa C beneficiaria de la publicidad en ningún momento había accedido a los datos, por lo que no existía cesión, señalando la sentencia que "como "ceder" es toda comunicación o revelación de datos, y constituye por tanto una acción, su apreciación no requiere que los datos pasen a formar parte de un fichero del cedente sino que es suficiente con que se traten dichos datos a favor del tercero y que este (el cesionario) trate dichos datos. En el presente caso, además, dicho tercero obtuvo un beneficio (publicidad de sus productos), pues según se desprende de las actuaciones y se recoge en los hechos probados de la resolución sancionadora: (A) suscribió un contrato con (B) por el cual aquella le permite la utilización de fichero de ex socios de (A) para la realización de campañas publicitarias de terceras empresas. Por lo que la entidad actora (A), responsable del fichero (y del tratamiento) de datos personales de ex socios, a través de la encargada del tratamiento (B) cedió los datos beneficiaria de la publicidad de la entidad actora por lo que tal pretensión ha de ser desestimada.

Por otra parte, se considera que la cesión no ha contado con el consentimiento de los afectados, teniendo en cuenta la cláusula dirigida a los mismos, con el siguiente tenor: "...Las finalidades del fichero son mantener relaciones con nuestros socios, antiguos

socios y demás interesados, poder remitirles información y ofertas sobre productos y servicios, adecuar éstos a sus intereses, necesidades y perfiles particulares así como a través del club o de otras entidades pertenecientes a la federación Española de Comercio Electrónico y Marketing Directo de la que (A) forma parte, poder remitirle publicidad u ofertas de otras entidades comerciales o de servicios que pudieran resultar de su interés; en especial, las referidas a la cultura y el ocio, productos y servicios para el hogar o de uso personal (electrodomésticos, textil, cosmética alimentación etc), automoción, inmobiliarios, aseguradores y financieros. También le informamos de la eventual cesión de sus datos a otras entidades de las que podría recibir ofertas, por escrito o en visitas personales, sin perjuicio del deber de círculo de lectores de cumplimentar, en este caso, cuanto pueda exigirse en cada momento en la normativa legal".

La Sentencia considera dicha cláusula contraria al artículo 11.3 LOPD, entendiendo que "dados los poco concretos términos de dicha leyenda, no es posible entender que exista información sobre finalidades determinadas y explícitas, ya que requiere, genéricamente, el consentimiento para el tratamiento de los datos para remitirles información y ofertas sobre productos y servicios, adecuar éstos a sus intereses, necesidades y perfiles particulares así como a través del Club o de otras entidades pertenecientes a la FECEMD", añadiendo que "la amplitud de categorías de bienes y servicios para los que se presta el consentimiento, además (publicidad u oferta de cualquier entidad comercial o de servicios "que pudieran resultar de su interés") tampoco permite al particular identificar de forma determinada y explícita las finalidades para las que serán tratados sus datos personales, en términos que le permitan prestar un consentimiento inequívoco como el exigido por la LOPD".

■ TRATAMIENTO DE DATOS CONTENIDOS EN GUÍAS DE COMUNICACIONES ELECTRÓNICAS

La SAN de 12 de julio de 2006 analiza un supuesto parcialmente similar al que acaba de describirse. El análisis jurídico de esta Sentencia resulta relevante en lo referente a la posibilidad de tratamiento de datos contenidos en las guías de comunicaciones electrónicas, consideradas como fuentes accesibles al público por el artículo 3 j) de la LOPD. Así se señala que los datos del denunciante figuraron en dicha guía hasta en día 22 de mayo de 2001 "por lo que a tenor de dicho artículo 28.3 LOPD los mismos pudieron utilizarse, al provenir de una fuente de acceso público, hasta el 22 de mayo de 2002", de forma que su utilización para la realización de un envío el 11 de marzo de 2003 "constituyó una cesión de datos, sin su consentimiento, ya que desde el 22 de mayo de 2002, la fuente de la que se obtuvieron dichos datos dejó de ser de acceso público". Asimismo, se aclara que no resulta admisible la alegación de la recurrente "aduciendo que el fichero en el que constaban dicho datos del afectado fue creado por ella en abril de 2002, lo cual a su juicio le permite la utilización de los repetidos datos dentro del período de un año desde tal creación del fichero, (hasta abril de 2003)", dado que dicha interpretación "carece de todo sustento legal, se opone a lo preceptuado con claridad en el repetido artículo 28.3 de la Ley 15/1999 y permitiría a cualquier entidad disponer de los datos a su libre y arbitraria voluntad".

■ TRATAMIENTO DE DATOS DE CLIENTES PARA LA CONTRATACIÓN DE UNA TARJETA.

La SAN de 12 de julio de 2006 se refiere al supuesto en que una entidad bancaria y otra aseguradora firman un acuerdo para la difusión entre los clientes de la segunda de la tarjeta emitida por la primera, a través de la red de agentes de la aseguradora que recabarán los datos de los clientes, comprobarán su veracidad y los remitirán a la entidad bancaria para la emisión de la tarjeta. En el caso de la afectada, los datos fueron rellenados directamente por el agente, constando determinados errores en los mismos y siendo la firma contenida en la solicitud completamente distinta de la correspondiente a la afectada. El recurso se refería únicamente a la entidad bancaria, aclarando que a la misma correspondía "adoptar las medidas de seguridad precisas para evitar que se realicen altas fraudulentas por los agentes (...) que comercializan la citada tarjeta y asegurarse de que la persona con la que contrata ha prestado el consentimiento -consentimiento que en el caso de autos no consta que hubiera prestado la interesada, al no reconocer como suya la firma obrante en la citada solicitud de tarjeta (...) y es quien dice ser. Al propio tiempo, se desestima la alegación de que la entidad aseguradora es encargada del tratamiento, debiendo aplicarse directamente lo dispuesto en el artículo 12.4 LOPD, toda vez que se indica que, dado que en este caso la aseguradora es, como encargada de promocionar la tarjeta "la que recaba datos personales de terceras personas cuya identidad se obligaba a comprobar y remite las solicitudes de la tarjeta a (...), que incorpora así los citados datos personales a sus ficheros y los trata", "no se trata de datos personales que estuvieran en el fichero de (...) y tuvieran que salir del mismo para ser conocidos y tratados por (...), sino de un supuesto distinto que no tiene encuadre en el citado precepto" (artículo 12 de la LOPD).

■ PRUEBA DE LA EXISTENCIA DE UN CONTRATO DE ENCARGADO DEL TRATAMIENTO

Las sentencias de 11 de enero y 25 de enero de 2006 se refieren a un supuesto en que se encontró abandonada en contenedores información referida a dos empresas que contenía datos de carácter personal, imponiéndose la consecuente sanción como consecuencia del tratamiento de datos de carácter personal sin la adopción de las adecuadas medidas de seguridad. La cuestión novedosa en este supuesto se refiere al hecho de que se alegó, respecto de los datos relacionados con una de las empresas, que los mismos eran tratados por la segunda en condición de encargada del tratamiento de la primera, para lo que se aportó el correspondiente contrato, de fecha 1 de febrero de 1999, en que se hacía referencia tanto a la LOPD como al Real Decreto 994/1999, de 11 de junio. De este modo, se apreció igualmente la existencia de una cesión de datos y un tratamiento indebido de datos por la cesionaria, recordando la primera de las sentencias citadas que "el "contrato aportado por la recurrente contiene una obvia irregularidad que hace dudar de forma muy fundada sobre su realidad y, por tanto, impide cualquier validez que al mismo se le quiere dar, especialmente para intentar con el mismo desvirtuar una conducta muy grave en materia de protección de datos de carácter personal pues según se recoge en su encabezamiento, es de fecha 1 de febrero de 1999, pero en sus cláusulas 6ª y 8ª se hace mención expresa a una normativa de protección de datos posterior (RD 994/1999, de 11 de junio)", añadiendo que "la recurrente, en su escrito de demanda, pretende justificar esa anomalía

alegando que, en realidad, hubo una novación del contrato, con la finalidad de adaptarlo a la nueva normativa de protección de datos, pero un error en la fecha del mismo. Sin embargo, esta alegación se ha de rechazar, por cuanto que una novación contractual, en tanto que constituye una sustitución de un contrato anterior por otro nuevo, exige, especialmente cuando el anterior se ha celebrado por escrito, que en el nuevo conste, también de forma expresa, ese nuevo acuerdo de voluntades y la fecha del mismo a los efectos de su validez; sobre todo en un caso como el de autos, en el que se pretende aplicar la excepción que el 12 de la LOPD prevé al principio general del consentimiento de los afectados".

■ CESIÓN DE DATOS PARA FINES NO PREVISTOS EN CLÁUSULA INFORMATIVA

La SAN de 12 de julio de 2006 analiza el supuesto en que un colegio de fisioterapeutas comunicó los datos de sus colegiados a una entidad formativa, en virtud de un convenio que suscribieron ambas entidades mediante el cual la primera remitía su base de datos de sus colegiados a dicha escuela a fin de que ésta exclusivamente enviara información a estos últimos sobre cursos de osteopatía, analizándose, en primer lugar, si dicho supuesto se encuentra amparado por el artículo 12 LOPD y, en caso contrario, si concurría el consentimiento inequívoco e informado de los afectados para la cesión a un tercero, tal y como exige el artículo 11.1 de la LOPD, en relación con los artículos 3, i) y 5 de dicho texto legal. Respecto de la primera cuestión, la Sentencia señala que "por mucho que la recurrente quiera ver de forma implícita en ese convenio dichas condiciones, lo cierto es que ese precepto legal es claro y no admite lugar a dudas de que exige que expresamente conste 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.; y también ha de constar las medidas de seguridad previstas en el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar", existiendo así una cesión de datos, que no contaba con el consentimiento de los afectados, dado que en la solicitud de inscripción colegial "no se puede concluir, como pretende la recurrente, que el afectado esté autorizando inequívocamente a su colegio para que éste pueda ceder esos datos personales a un tercero para una concreta finalidad, pues lo único que se dice en ambos textos es que al colegio se le ceden esos datos para que éste los utilice, no para que los ceda a un tercero, con temas relacionados con la fisioterapia".

■ NOTIFICACIÓN DE INCLUSIÓN EN FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO

La SAN de 31 de mayo de 2006 analiza el supuesto en que la AEPD sancionó en fecha 10 de diciembre de 2004 a una entidad de solvencia patrimonial y crédito por no haber acreditado suficientemente la notificación de inclusión en el fichero de los datos del denunciante, entendiéndose que la notificación de la inclusión de los datos personales en el fichero debe acreditarse no solo por su envío sino también por su recepción, no habiendo quedado ésta acreditada.

La Sentencia recuerda que "la Agencia de Protección de Datos venía considerando que la inclusión en el fichero (...) de la realización de una comunicación al afectado por el tratamiento de sus datos acreditaba suficientemente su realización", sin embargo "en la resolución que ahora se recurre cambia dicho criterio con fundamento en dos sentencias de este Tribunal, y procede a sancionar (...), por considerar no acreditada la notificación a que estaba obligada con arreglo al expresado artículo 29 de la Ley 15/1999".

La Sentencia considera la existencia de indicios suficientes para estimar el recurso, dado que "en el Informe de actuaciones de la Inspección de Datos se recoge que la inspección efectuada en la entidad (...) constató la existencia de una carta enviada a nombre de (el denunciante) y dirigida a la dirección (...), no constando dicha carta como devuelta". Añade así que "la parte actora aporta diversos indicios que apuntan a la realización de la comunicación. Por un lado, como ya hemos visto, la inclusión en el fichero auxiliar de NOTIFICACIONES (...) de esta comunicación como realizada; por otro, el hecho de que (el denunciante) se dirige a (...) sabiendo que sus datos están incluidos en el fichero (...) y quien había sido la entidad informante de los mismos (circunstancia que se recoge en la propia resolución administrativa) sin que se haya acreditado mínimamente que dicho conocimiento lo obtuvo de forma distinta de la comunicación que dice haber realizado (...), y, finalmente, el hecho de que al domicilio al que aparece dirigida la comunicación que se niega haber recibido, se han remitido otras comunicaciones de las que el denunciante ha tenido perfecto conocimiento".

En consecuencia, la Audiencia Nacional viene a considerar suficiente la acreditación de la notificación efectuada a través de la aportación de indicios en este sentido, tomando en consideración el principio de valoración conjunta de la prueba.

■ TRATAMIENTO DE DATOS RELACIONADO CON LA CONTRATACIÓN TELEFÓNICA

La SAN de 31 de mayo de 2006 se refiere a un supuesto en que le fue denegada a la denunciante la empresa prestadora una solicitud de alta en un servicio, informándole de que sus datos se encontraban en un fichero de impagados y que existe otra persona con otro nombre y con su mismo número de DNI incluido en un fichero de incumplimiento de obligaciones dinerarias, habiendo sido introducido ese dato en el fichero por la recurrente que, sin embargo, no acreditó la existencia de la relación contractual entre la misma y dicha segunda persona. De este modo, se había incluido erróneamente el dato del DNI de la recurrente en el fichero, sin constar que la entidad informante había adoptado las medidas necesarias para acreditar que el DNI no correspondía al de su cliente, respecto del que además no podía acreditar la celebración del contrato. La Sentencia toma en consideración lo dispuesto en el artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, así como en el artículo 5 del Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica cuyo artículo. Asimismo, recuerda la doctrina de la Sala según la cual "es el responsable del tratamiento (por todas, sentencia de esta Sala de 25 de octubre de 2002 Rec. 185/2001) a quien corresponde asegurarse de que aquel a quien se solicita consentimiento, efectivamente lo da, y que esa persona que está dando el consentimiento es efectivamente el titular de esos

datos personales, debiendo conservar la prueba del cumplimiento de la obligación a disposición de la Administración, encargada de velar por el cumplimiento de la Ley", concluyendo que "resulta, por tanto, que tal la empresa demandante no sólo no ha aportado ningún elemento probatorio que acredite la celebración telefónica del contrato, sino que tampoco ha acreditado el cumplimiento de las garantías y cautelas que determinan las normas transcritas. Más concretamente, no consta justificación documental, ni cinta de grabación, ni cualquier otro soporte que justifique la celebración del contrato, y tampoco hay constancia del ulterior envío y recepción por el destinatario de la documentación correspondiente al mencionado contrato", por lo que procede la imposición de la sanción.

SENTENCIAS DE MAYOR RELEVANCIA DICTADAS POR EL TRIBUNAL SUPREMO

Como ya se indicó con anterioridad, el criterio sostenido por la Agencia Española de Protección de Datos ha sido mantenido en la práctica totalidad de las sentencias dictadas por el Tribunal Supremo durante el año 2006, declarándose haber lugar a un recurso interpuesto contra la sentencia de la AN confirmatoria de la resolución dictada por la Agencia, exclusivamente en lo que se refiere a la reducción de la cuantía de la sanción. Igualmente se declaró no haber lugar al recurso interpuesto por la representación procesal de la Agencia contra la Sentencia de la AN que declaró ilegales determinados preceptos de la Instrucción 1/2000.

Tal y como sucedía en el año 2005, y a diferencia de lo ocurrido en años anteriores, en que la mayor parte de la jurisprudencia del Tribunal Supremo se refería a supuestos muy concretos, reiterándose en varios fallos a lo largo del ejercicio, durante el año 2006 han sido variadas las cuestiones sobre las que se ha pronunciado el Alto Tribunal, siendo preciso referirnos a la mayor parte de los casos, habida cuenta del interés que presentan y de la naturaleza del Órgano Jurisdiccional que dicta las sentencias.

■ TRATAMIENTO DEL DATO DE IDEOLOGÍA

La STS de 25 de enero de 2006 confirma la SAN de 28 de septiembre de 2001. En este caso, una determinada empresa hostelera trató el dato de ideología de un determinado cargo público, remitiéndole una invitación en cuyo sobre constaban las siglas del partido político al que se suponía que se encontraba afiliado el afectado. La Sala vuelve a poner de manifiesto la diferencia entre los derechos fundamentales a la intimidad y a la protección de datos, recordando la doctrina derivada de la STC 292/2000, de 30 de noviembre, por lo que recuerda que "resulta en absoluto irrelevante, a los efectos de este motivo de casación, la invocada publicidad sobre la pertenencia del denunciante al partido (...) así como las manifestaciones del mismo dirigidas a la Agencia de Protección de Datos o el resultado de la cuenta de pérdidas y ganancias de la empresa sancionada". A su vez, la Sala analiza la apreciación de culpabilidad en el presente caso,

indicando que "el elemento culpabilístico del tipo sancionador aplicado concurre cuando se incluye el expresado dato sobre la ideología, no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado, cuya circunstancia puede ser relevante en el momento de determinar la graduación de la pena, concurriendo, por tanto, los requisitos exigibles para que la conducta sea culpable, sin que se esté ante un supuesto de error, como alega la recurrente, ya que la Ley exige, cuando se tratan datos automatizadamente, conocer su régimen jurídico, debiendo abstenerse de incluir datos sobre la ideología de la persona sin su consentimiento expreso, incurriendo en una falta de diligencia que determina la existencia de culpa y, con ello, en la comisión del lícito administrativo que la hizo acreedora de sanción"

■ NECESIDAD DE CONTRATO ESCRITO PARA LA EXISTENCIA DE ENCARGADO DEL TRATAMIENTO

La STS de 13 de septiembre de 2006 desestima el recurso interpuesto contra la SAN de 16 de febrero de 2005, al considerar que no concurren los requisitos necesarios para la interposición del recurso de casación para la unificación de doctrina. La Sentencia hace suyo el razonamiento de la Sentencia de instancia en relación con la ratio decidendi del proceso, al señalar que "para que concurra la figura del encargado del tratamiento el artículo 12.2 requiere, ya lo hemos señalado, que la relación entre el responsable del fichero y ese tercero al que se confiere el encargo quede regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido y que deberá incluir las especificaciones que el propio precepto legal determina", concluyendo que "tanto si atendemos a las estipulaciones del contrato de arrendamiento de servicios que A y B suscribieron (...) como si examinamos las cláusulas de los pliegos de condiciones específicas y generales que figuran adjuntos al contrato (...) comprobamos que no se contienen allí las especificaciones y prevenciones que exige el mencionado artículo 12.2 de la Ley Orgánica 15/99, pues no estando concretado en tales documentos el contenido ni la finalidad del fichero o ficheros que se ponen a disposición de A tampoco incorporan el compromiso expreso por parte de esta entidad de no aplicar o utilizar los datos con un fin distinto al estipulado, ni especifican, en fin, las medidas de seguridad que A, SL habría de establecer".

■ PRESTACIÓN DE SERVICIOS DE "SCORING"

La STS de 1 de marzo de 2006 desestima el recurso interpuesto contra la SAN de 18 de enero de 2002, que confirma la sanción impuesta por la AEPD a una entidad como consecuencia de la contratación de un servicio de "scoring" de sus clientes, consistente en la comunicación por parte de aquélla de los datos de sus clientes a una tercera empresa perteneciente al sector del estudio de la solvencia patrimonial y crédito, a fin de que por la misma se considere si dichos clientes son "aptos" o "no aptos", en función bien de los datos facilitados por los propios interesados, bien de los que la propia destinataria tiene en su poder. La Sentencia insiste en el criterio sustentado en otras de la Sala en relación con el requisito de forma escrita para la contratación de un encargado del tratamiento, teniendo en cuenta que los hechos se

produjeron durante la vigencia de la LORTAD. Así, se señala que "sin negar el principio general de perfección del contrato por el simple consentimiento (artículo 1258 del Código Civil), que tampoco niega la sentencia recurrida, es de hacer notar que, de los términos en que está redactado el contenido del artículo 27 que se alega como vulnerado, expresamente resulta la necesidad de que conste plasmado por escrito el fin del contrato de servicios, pues a ello alude y se refiere dicho texto legal cuando prohíbe aplicar o utilizar los datos obtenidos por un tercero "con fin distinto al que figure en el contrato de servicios", lo que evidentemente hace referencia a la necesidad de plasmar por escrito ese fin determinante de la cesión para así excluir la responsabilidad en el cesionario". Se considera así probada la existencia de una cesión de datos que no resulta amparada por la cláusula informativa contenida en los contratos de prestación de servicios, dado que sus términos "no permiten entender comprendida dentro de la misma la cesión de datos para efectuar una prueba de scoring o establecimiento de riesgo de clientes, puesto que ello es ajeno a la finalidad para la que le fueron facilitados a (...) los datos personales de sus clientes para la prestación del servicio contratado con (...), lo que no facultaba a ésta para su cesión a tercero para el tratamiento de dichos datos para la evaluación del riesgo de los clientes, pues ello afecta a la privacidad de los mismos, como correctamente apreció la sentencia recurrida, al efectuarse una valoración que puede dibujar un determinado perfil de su persona o configurar una determinada reputación o fama que es, en definitiva, expresión del honor por lo que la cesión exigía el consentimiento expreso de los afectados".

■ TRATAMIENTO DE DATOS BANCARIOS DE LOS AFECTADOS POR UNA EMPRESA CON QUE CONTRATAN UN SERVICIO

La STS de 27 de abril de 2006 declara no haber lugar al recurso de casación para la unificación de doctrina interpuesto contra SAN de 3 de noviembre de 2004, al no haberse cumplido los requisitos necesarios para la interposición del recurso. La empresa sancionada obtenía de otras los datos personales relativos a cuentas bancarias de sus clientes, almacenando en su sistema informático información acerca de la cuenta bancaria del cliente. Se señalaba por la recurrente que una condición general de su contrato le permite comprobar la solvencia del cliente mediante el acceso a ficheros en los que los datos se hayan obtenido de conformidad con el art. 28 de la LO 5/92. La Sala declara que ello no legitima el tratamiento, dado que dicha cláusula no habilita para que sean incorporados a los ficheros de la actora otros datos distintos a los de solvencia, obtenidos por terceras empresas y que los datos que dicha entidad incorpora a sus ficheros, facilitados por las citadas empresas, no se refieren al cumplimiento o incumplimiento de obligaciones dinerarias ni consta que procedan de fuentes accesibles al público ni que hayan sido obtenidos con el consentimiento de los interesados.

■ CESIÓN DE DATOS PARA LA EMISIÓN DE UNA TARJETA SIN CONSENTIMIENTO

La STS de 7 de febrero de 2006 confirma la de la AN de 8 de junio de 2001 por la que se confirmaba a su vez la sanción de la AEPD como consecuencia de la celebración entre una entidad financiera y una federación deportiva de un contrato de colaboración para la emisión de una tarjeta a los federados, para lo cual la segunda cedió a la

primera la relación de federados disponibles, en soporte magnético. Se alegaba por la federación sancionada que la cesión sólo se refería a fuentes accesibles al público, por lo que no se infringía la entonces vigente LOPRTAD, considerándose por la Sala que dicha alegación no debía prosperar, al facilitarse implícitamente el dato de "federado", que no aparece recogido en ninguna de esas fuentes. Al propio tiempo, la Sala desestima la alegación de que no se produce quiebra alguna de la intimidad de los afectados, al poner de relieve el carácter autónomo del derecho a la protección de datos frente al derecho a la intimidad, tal y como ha consagrado la STC 292/2000, de 30 de noviembre.

■ INCLUSIÓN DE DATOS EN LA CENTRAL DE INFORMACIÓN DE RIESGOS DEL BANCO DE ESPAÑA

La STS de 21 de febrero de 2006 se refiere al recurso de casación interpuesto contra SAN de 18 de mayo de 2001, en la que se desestima el recurso interpuesto contra Resolución de la AEPD de 22 de abril de 1999 en la que se declaraba la ausencia de responsabilidad del Banco de España, en relación a una denuncia presentada por el actor en la que se hacía constar que en la Central de Información de Riesgos del Banco de España figuraban indebidamente datos relativos a su persona, alegando que el Banco de España no les habría notificado la inclusión de sus datos en el fichero y que dicho Banco no contestó al escrito que le habían remitido, solicitándole el acceso a los datos referidos a ellos. La Sentencia confirma lo señalado en instancia, aclarando en primer lugar que la CIRBE no es un fichero de los regulados especialmente por el artículo 28 de la LORTAD (y 29 de la LOPD), al tratarse de un fichero de titularidad pública. Al propio tiempo, frente a la alegación de no haberse recibido información alguna en relación con la inclusión, el TS acepta la existencia de indicios en sentido contrario, apreciada en instancia, al recordar que el recurrente tenía conocimiento de su incidencia en la CIRBE y de la identidad de la entidad financiera informante, lo que "resulta imposible", dado que en la información facilitada desde el registro CIRBE no consta la identificación de la entidad acreedora, "de lo que se infiere que la única forma de que el recurrente haya tenido conocimiento de dicho extremo es porque ha recibido la comunicación en el domicilio a la que fue enviada".

■ RESPONSABLE DEL FICHERO Y RESPONSABLE DEL TRATAMIENTO

La STS de 18 de julio de 2006 se refiere a un supuesto de inclusión de un dato erróneo en un fichero referido al cumplimiento o incumplimiento de obligaciones dinerarias, toda vez que el dato derivado de la deuda contraída por el uso de una tarjeta de crédito fue comunicado por el acreedor al fichero común con posterioridad a tener conocimiento de la denuncia presentada por la titular de la tarjeta por la sustracción de la misma en fecha anterior a aquella en que se contrajo la deuda. La Sala, reiterando la doctrina mantenida en anteriores Sentencias, considera no aplicable la doctrina derivada de las sentencias de 29 de julio y 3 de diciembre de 2002, como consecuencia de la nueva regulación contenida en la LOPD de las figuras del responsable del fichero y el responsable del tratamiento.

■ DETERMINACIÓN DE LA CUANTÍA DE LA SANCIÓN

La STS de 7 de marzo de 2006 declaró haber lugar al recurso interpuesto contra la SAN de 5 de octubre de 2001, frente a resolución de la AEPD por la que se imponía a la recurrente una sanción como consecuencia de la comisión de una infracción grave prevista en el artículo 43.3 d) de la LORTAD como consecuencia de la utilización del censo electoral para la realización de actividades de publicidad y prospección comercial, imponiéndose dicha sanción en una cuantía de treinta millones de pesetas, como consecuencia de la reincidencia del sancionado en su actividad. La sentencia reitera, de conformidad con la jurisprudencia ya consolidada, en la materia, a partir de la STS de 18 de octubre de 2000, la procedencia de imposición de una sanción, al resultar contrario a la legislación de protección de datos la utilización del censo con los fines citados; del mismo modo, considera que no procede la aplicación en este caso del principio non bis in idem, al referirse este supuesto a la utilización de datos de distintos ciudadanos que los enjuiciados en sentencias y resoluciones anteriores. Igualmente, siguiendo la jurisprudencia de la Sala, considera que no procede la aplicación al caso de lo dispuesto en el artículo 45.5 LOPD. No obstante, sí se considera que debe modularse el importe de la sanción, por aplicación del artículo 45.4 de la propia Ley, al haberse apreciado para la determinación de su cuantía la existencia de reincidencia, siendo así que la resolución hacía referencia a un único expediente tramitado con anterioridad. En consecuencia, se acuerda la reducción de la sanción de treinta a veinte millones de pesetas.

■ VALOR PROBATORIO DE LAS ACTAS DE INSPECCIÓN

La STS de 17 de octubre de 2006 desestima el recurso interpuesto contra la SAN de 12 de abril de 2002, en que se había considerado contraria a la LOPD la cesión de datos por parte de una empresa a un determinado sindicato representativo en la misma de un CD-ROM con los datos de los trabajadores, habiendo el mismo sido empleado para la difusión de acciones formativas por parte de una entidad dependiente del propio sindicato. La doctrina de la Sentencia resulta relevante en cuanto se consideró que la comunicación únicamente había quedado acreditada a través de presunciones, dudándose del valor probatorio de las actas de inspección. A tal efecto, se recuerda la jurisprudencia del propio Tribunal en este sentido, señalándose que "las declaraciones contenidas en las actas, sin duda, tienen valor probatorio pues gozan de la presunción de que dichas declaraciones se hicieron ante el inspector, otra cosa será si dicha declaración es o no verdadera" y que "es también reiterada la jurisprudencia de este Tribunal que ha limitado el valor atribuible a las Actas de la Inspección, limitando la presunción de certeza a solo los hechos que por su objetividad son susceptibles de percepción directa por el Inspector, o a los inmediatamente deducibles de aquéllos o acreditados por medios de prueba consignados en la propia acta como pueden ser documentos o declaraciones incorporadas a la misma (Sentencia de 24 de junio de 1991)", considerando que "es lícito, por lo tanto, partir del hecho de que en intermediación, y ante el inspector, se reconoció que la empresa había entregado un disquete con los datos".

■ RECURSO REFERENTE A LA INSTRUCCIÓN 1/2000 DE LA AEPD SOBRE MOVIMIENTOS INTERNACIONALES DE DATOS

La STS de 25 de septiembre de 2006 declara no haber lugar al recurso interpuesto por la Abogacía del Estado, en representación de la Agencia, contra la SAN de 15 de marzo de 2002 en cuya parte dispositiva se señalaba que "FALLAMOS. Que estimando en parte el recurso Contencioso-Administrativo interpuesto en representación de (...) contra la Instrucción 1/2000, de 1 diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, debemos anular y anulamos el apartado 2/ de la Norma Tercera y la Norma Sexta de dicha Instrucción, si bien ambos únicamente en cuanto pretenden extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción del artículo 34 de la Ley Orgánica 15/1999, y anulamos también el apartado 1/ de la Norma Cuarta de la misma Instrucción, desestimando en lo demás la pretensión de la demandante, sin imponer las costas de este proceso a ninguno de los litigantes".

La STS analiza la cuestión en su Fundamento de Derecho Quinto, que reproducimos a continuación:

"Para la resolución del único motivo de recurso formulado resulta preciso tener en cuenta que la Sala de instancia no anula las Normas 3ª.2; 4.1 y 6ª de la Instrucción 1/2000 (RCL 2000, 2875), sino que las anula solo en cuanto pretendan extender su aplicación a los supuestos en que la Ley Orgánica 15/99 (RCL 1999, 3058) en su art.34 ha dispuesto que no procede la aplicación del art. 33, precepto este que en relación al movimiento internacional de datos establece limitaciones y controles, tal y como antes se ha transcrito.

La conclusión resulta lógica: en los supuestos en los que la propia Ley fija excepciones en relación a las limitaciones y controles, la Instrucción de la Agencia, que tiene por objeto el desarrollo de la práctica y ejecución de estos, no poder ser de aplicación lo que es una consecuencia obligada del tenor del art. 34 de la Ley Orgánica 15/99.

El propio Abogado del Estado incurre en contradicciones en su recurso, pues después de alegar la vulneración de aquellos preceptos antes expuestos, con especial referencia al art. 34 de la Ley, hace como antes se ha dicho una consideración peculiar, señalando que es "inaceptable el prevailecimiento absolutamente incondicionado de los supuestos previstos en el art. 34 de la LO cuya efectividad debe estimarse implícitamente subordinada a la demostración de su realidad y certeza".

No solo parece en su argumentación pretender sostener que no ha de estarse a unas excepciones al régimen de autorización para la transferencia internacional de datos que la propia LO 15/99 permite, sino que tampoco concreta, como hubiera sido necesario atendido el carácter extraordinario del recurso de casación y el principio de especialidad de los motivos, cuales son las precisas vulneraciones que imputa, sino que unciamente razona: que "la sala "a quo" aplica, a nuestro juicio inadecuadamente, los principios y normas sobre los que descansa el sistema administrativo de protección de datos, interpretando que la mera afirmación por el transferente de hallarse en un supuesto de excepción ha de reputarse verosímil y fidedigna".

Si la propia Ley Orgánica 15/99 en su art.34, tal y como ya había regulado el art. 26 de la Directiva 95/46 CE (LCEur 1995, 2977), establece unas excepciones en cuanto al control del Director de la Agencia de Protección de Datos en las transferencias internacionales de datos, debe concluirse que la Sentencia recurrida no vulnera ninguno de los preceptos recogidos por el Abogado del Estado, sino que hace una aplicación lógica y obligada del art. 34 LO referido, ya que no cabe aplicar unas determinadas normas de la Instrucción, en cuanto contravienen el tenor de la Ley, no siendo en tal sentido asumible la argumentación del Abogado del Estado que parece pretender una primacía de la Instrucción sobre la Ley Orgánica, lo que a todas luces resulta contrario al principio de jerarquía normativa."

LA INSTRUCCIÓN 1/2006, DE 8 DE NOVIEMBRE, DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, RELATIVA AL TRATAMIENTO DE DATOS PERSONALES CON FINES DE VIGILANCIA A TRAVÉS DE SISTEMAS DE CÁMARAS O VIDEOCÁMARAS

ANÁLISIS GENERAL

"El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica"

Con estas palabras comienza la Exposición de motivos de la Instrucción 1/2006 de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Esta Instrucción ha pretendido otorgar mayor claridad y por ende seguridad jurídica en un campo que carece de una regulación, acorde a las necesidades que vive la sociedad actual.

Sin embargo, no podemos perder de vista que el objetivo de la Instrucción, se centra única y exclusivamente en el ámbito de la protección de datos de carácter personal, y es desde esa perspectiva desde donde hay que analizarla.

La Agencia como órgano encargado de velar por la protección del derecho fundamental a la protección de datos de carácter personal, tuvo constancia de las incógnitas que la videovigilancia generaba en este punto. Por tanto partiendo de la base de que las imágenes son datos personales, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4. del Real Decreto 1322/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica y en consecuencia todas las imágenes captadas por las miles de cámaras que nos rodean debían de cumplir con la LOPD, la Agencia decidió que para aclarar dichas dudas y haciendo uso de su capacidad normativa, debía de dictar una Instrucción.

En la regulación de esta Instrucción se ha tenido en cuenta que la seguridad y la vigilancia, son elementos presentes en la sociedad actual, y que no tienen que ser incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos.

La delimitación del ámbito objetivo en la Instrucción resulta esencial, dado que concreta que tan sólo resultará aplicable a las imágenes obtenidas con fines de vigilancia de personas identificadas e identificables, siempre que para identificarlas no sean necesarios esfuerzos desproporcionados, lo que excluye de inmediato aquellas grabaciones que en ningún momento permitan identificar a las personas.

Continúa describiendo que el tratamiento de las imágenes puede consistir en la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas. Esta descripción detallada sobre lo que se entiende tratamiento en videovigilancia resulta especialmente aclaratoria, dado que algunas consultas habían planteado que la simple reproducción en tiempo real no era tratamiento y por tanto estaban excluidas de la Ley Orgánica 15/1999. Así, indicar que la simple reproducción a tiempo real genera un tratamiento supone una aclaración a todos aquellos que entendían que quedaba excluido, lo que no genera la reproducción a tiempo real es un fichero como se hace constar en el artículo 7.

La Instrucción excluye de su ámbito de aplicación a las imágenes que un particular pueda captar en el ámbito de su vida privada y familiar y las obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad que se regirá por su regulación específica sobre la materia.

Otro punto especialmente importante es el relativo a la legitimación para el tratamiento, pieza angular en materia de protección de datos. El tratamiento que se realice por una cámara deberá encontrarse legitimado por alguno de los supuestos previstos en la LOPD. Ello exigirá, en general, que se cuente con el consentimiento de cada uno de los que resulten grabados, cosa que resulta en la práctica imposible o que una ley legitime dicho tratamiento. A tal efecto, entendemos que tanto la Ley de Seguridad Privada como y la Ley Orgánica de Seguridad Ciudadana habilitan el tratamiento, mediante el cumplimiento de sus requisitos, todo ello sin olvidar que además las instalaciones deberían de respetar la legislación vigente en materia de seguridad.

Asimismo, cabe destacar por su importancia la necesidad de cumplir con la obligación de informar a los ciudadanos para que puedan conocer cuando se encuentran en alguna zona videovigilada. Por ello es fundamental que se cumpla con este requisito, que no es sino una exigencia legal derivada del artículo 5 de la LOPD. La ubicación del cartel informativo, en un lugar suficientemente visible, no implica que debajo de cada cámara se coloque este cartel, basta si se graba el interior de un edificio que se ubiquen los carteles en la entrada a los mismo.

En conclusión, esta Instrucción ha pretendido poner de manifiesto que nuestra imagen nos pertenece y ello sin olvidar que las cámaras generan seguridad y ayuda en situaciones delictivas, pero un uso proporcionado de las mismas nos beneficia a todos, así se hace constar en la Exposición de motivos de la citada Instrucción *"la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona."*

LEGITIMACIÓN PARA EL TRATAMIENTO

En primer lugar es preciso describir los siguientes tratamientos de imágenes y analizar la legitimación que ha de concurrir en cada uno de estos supuestos:

- Imágenes grabadas por las Fuerzas y Cuerpos de Seguridad del Estado:
 - En el acceso a edificios públicos.
 - En el acceso a edificios privados.
 - En la vía pública.
- Imágenes grabadas por servicios de seguridad privada:
 - En edificios públicos
 - En edificios privados.
 - En la vía pública.
- Imágenes grabadas por empresas de servicios (no de seguridad).
 - En edificios privados.
 - En la vía pública.
- Imágenes grabadas por el empresario en el centro de trabajo.
 - Grabación de imágenes de trabajadores.
 - Grabación de imágenes de clientes o consumidores, sin que exista vínculo jurídico entre el empresario y el cliente.
- Imágenes grabadas para uso doméstico
- Imágenes grabadas en otros recintos.
 - En recintos privados. (interior de aparcamiento o urbanizaciones cerradas..)
 - En la vía pública.
- Imágenes grabadas por vigilancia de tráfico

■ SUPUESTOS A ANALIZAR

De la enumeración realizada, deben excluirse a los efectos de su regulación, y así se efectúa por parte de la Instrucción, los tratamientos de imágenes grabadas para uso doméstico, al resultar de aplicación lo dispuesto en el artículo 2.2 a) LOPD.

Igualmente, dado lo dispuesto en el artículo 2.3 de la LOPD se regirá por su legislación específica el tratamiento de datos de imágenes llevado a cabo por las Fuerzas y Cuerpos de Seguridad del Estado, regido por la Ley Orgánica 4/1997, aplicable, según su artículo 1 a "la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública", y así se hace constar en el artículo 1.3 de la Instrucción.

Por último, dado que pretende limitarse el alcance de la Instrucción al tratamiento de datos de imágenes con fines de videovigilancia, entendida esta como la protección de la seguridad en recintos abiertos o cerrados, debe también excluirse el tratamiento de datos efectuado para la vigilancia del tráfico. En este sentido, la disposición adicional octava de la LO 4/1997 se refiere a este tipo de supuestos como "La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico", pudiendo considerarse que la finalidad referida no es coincidente con la que se prevé en el ámbito de la Instrucción.

A continuación, se analizarán los supuestos referidos al tratamiento de datos en el entorno laboral, y los relacionados con la normativa reguladora de la seguridad ciudadana y de la seguridad privada, a fin de poder enumerar los supuestos en los que exista una norma con rango de Ley habilitante del tratamiento.

■ TRATAMIENTO DE DATOS POR EMPRESAS DE SEGURIDAD

En relación con el tratamiento de imágenes por parte de las empresas de seguridad privada, debe tenerse en cuenta, en primer lugar, lo dispuesto en la Ley 23/1992, de 30 de julio, de Seguridad Privada (en lo sucesivo LSP), que regula, según su artículo 1.1 "la prestación por personas, físicas o jurídicas, privadas de servicio de vigilancia y seguridad de personas o de bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de seguridad pública".

Asimismo, añade el artículo 1.2 que "A los efectos de la presente Ley, únicamente pueden realizar actividades de seguridad privada y prestar servicios de esta naturaleza las empresas de seguridad y el personal de seguridad privada, que estará integrado por los vigilantes de seguridad, los jefes de seguridad y los escoltas privados que trabajen en aquéllas, los guardas particulares del campo y los detectives privados", sin perjuicio de las especialidades que se analizarán posteriormente, previstas en las normas reguladoras, en general, de la seguridad ciudadana.

El artículo 5.1 e) de la LSP dispone que "con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollen, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades (...) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad". Esta previsión se reitera en el artículo 1 del Reglamento de Seguridad Privada, aprobado por Real decreto 2364/1994, de 9 de diciembre (en lo sucesivo RSP).

De este modo, la Ley habilita que los sujetos previstos en su ámbito de aplicación puedan instalar dispositivos de seguridad, entre los que podrían encontrarse las cámaras, siempre con la finalidad descrita en el citado artículo 1.1.

Para la efectiva puesta en funcionamiento de la medida, el artículo 6.1 dispone que "los contratos de prestación de los distintos servicios de seguridad deberán en todo caso consignarse por escrito, con arreglo a modelo oficial, y comunicarse al Ministerio del Interior, con una antelación mínima de tres días a la iniciación de tales servicios".

El artículo 20 del RSP regula el procedimiento de notificación del contrato, la autoridad competente y el régimen aplicable a la contratación del servicio por las Administraciones Públicas y a supuestos excepcionales que exijan la inmediata puesta en funcionamiento del servicio.

Por último, el artículo 7.1 establece que "Para la prestación privada de servicios o actividades de seguridad, las empresas de seguridad habrán de obtener la oportuna autorización administrativa mediante su inscripción en un Registro que se llevará en el Ministerio del Interior".

La inscripción se regula en el artículo 2 del RSP, detallando el Anexo los requisitos que han de reunir estas empresas. No obstante, quedarían excluidas las de ámbito exclusivamente autonómico. Además, el artículo 39.1 dispone que "únicamente podrán realizar las operaciones de instalación y mantenimiento de sistemas de seguridad electrónica contra robo e intrusión y contra incendios las empresas autorizadas".

En consecuencia, siempre que se haya dado cumplimiento a los requisitos formales establecidos en los artículos precedentes (inscripción en el Registro de la empresa y comunicación del contrato al Ministerio del Interior), las empresas de seguridad reconocidas podrán instalar dispositivos de seguridad, entre los que se encontrarían los que tratasen imágenes con fines de videovigilancia, existiendo así una habilitación legal para el tratamiento de los datos resultantes de dicha instalación.

De este modo, quedaría legitimado por la existencia de una norma con rango de Ley habilitante el tratamiento al que se refiere el apartado 2 de los citados con anterioridad, siempre que se cumplan los requisitos a los que se ha hecho referencia o concurra una de las excepciones previstas en el RSP, no siendo necesario el consentimiento del afectado.

■ OTROS TRATAMIENTOS EN ESTABLECIMIENTOS, LOCALES O EDIFICIOS Y SUS ALREDEDORES

En los supuestos en los que la instalación y tratamiento de las imágenes no se realiza por una empresa de seguridad privada, no existe, con carácter general, una norma legal habilitante del tratamiento de las imágenes. No obstante, el artículo 13 de la Ley Orgánica 1/1992, de Seguridad Ciudadana (en adelante LOSC) dispone que "El Ministerio del Interior podrá ordenar, conforme a lo que se disponga reglamentariamente, la adopción de las medidas de seguridad necesarias en establecimientos e instalaciones industriales, comerciales y de servicios, para prevenir la comisión de los actos delictivos que se puedan cometer contra ellos, cuando generen riesgos directos para terceros o sean especialmente vulnerables".

Como señala la propia Exposición de Motivos del RSP, el mismo no sólo desarrolla las previsiones de la LSP, sino también de la propia LOSC. Así, se indica que "Por lo que respecta a la seguridad en establecimientos e instalaciones, se desarrolla el artículo 13 de la Ley Orgánica sobre Protección de la Seguridad Ciudadana, determinando los servicios y sistemas de seguridad que habrán de adoptar las distintas clases de establecimientos, a cuyo efecto se cuenta con la experiencia acumulada durante los últimos años, adecuándose las medidas de seguridad en entidades y establecimientos públicos y privados al objeto perseguido, teniendo en cuenta las nuevas tecnologías".

Pues bien, el Título III del RSP regula esta materia, señalando con carácter general su artículo 111.1 que "De acuerdo con lo dispuesto en el artículo 13 y en la disposición adicional de la Ley Orgánica 1/1992, sobre protección de la seguridad ciudadana, y con la finalidad de prevenir la comisión de actos delictivos, la Secretaría de Estado de Interior, para supuestos supraprovinciales, o los Gobernadores Civiles podrán ordenar que las empresas industriales, comerciales o de servicios adopten las medidas de seguridad que, con carácter general o para supuestos específicos, se establecen en el presente Reglamento". Además, el artículo 112.1 dispone que "cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes".

Entre dichas medidas se encuentra, según el artículo 112.1 c) la "instalación de dispositivos y sistemas de seguridad y protección", pudiendo asimismo ordenarse la creación en la empresa de un departamento de seguridad (artículo 112.1 a) que, según el artículo 116 tendrá entre otras misiones la de "control del funcionamiento de las instalaciones de sistemas físicos y electrónicos, así como del mantenimiento de éstos y la gestión de las informaciones que generen".

El capítulo III establece medidas específicas para determinado tipo de actividades. Dentro de las mismas, la Sección 1ª se refiere a los "bancos, cajas de ahorro y demás instituciones de crédito", señalando el artículo 120.1 a) que "En los establecimientos u

oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso teniendo en cuenta las circunstancias enumeradas en el artículo 112 de este Reglamento y los criterios que se fijen por el Ministerio de Justicia e Interior, oyendo a la Comisión Mixta Central de Seguridad Privada (...) Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquéllos, y que habrán de funcionar durante el horario de atención al público, sin que requieran la intervención inmediata de los empleados de la entidad".

En los restantes supuestos regulados por el RSP no se establece expresamente esta medida, sin perjuicio de lo dispuesto en las normas generales del Título III a las que se acaba de hacer referencia.

De este modo, la instalación de dispositivos de videovigilancia por parte de las entidades de crédito se encontraría habilitada por el artículo 13 de la LOSC, por lo que el tratamiento de imágenes por los mismos se encuentra amparado por una norma con rango de Ley.

En los restantes supuestos, debería estarse a la existencia de una decisión específica en relación con establecimientos de un sector concreto o establecimientos concretos, bien de una determinada área, bien en particular. En ese caso, el tratamiento se encontraría amparado por el ya citado artículo 13.1 LOCS.

De no existir una de las dos habilitaciones ya citadas, basadas en la LOSC no existe norma con rango de Ley que otorgue cobertura al tratamiento, por lo que al no ser de aplicación los supuestos previstos en el artículo 6.2 LOPD, sería preciso contar con el consentimiento de los afectados.

■ TRATAMIENTO EN EL LUGAR DE TRABAJO

Por último, en cuanto al tratamiento de datos de imágenes en el lugar de trabajo, el artículo 20.3 del Estatuto de los Trabajadores (en adelante ET) dispone que "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".

Por otra parte, se tiene conocimiento de la doctrina del Tribunal Supremo, en virtud de la cual dichas medidas deben haber sido hechas constar expresamente al trabajador, pasando así a formar parte de la propia relación laboral y siendo el tratamiento de los datos necesario para su adecuado desenvolvimiento.

Es preciso tener en cuenta en esta materia lo dispuesto en La Sentencia del Tribunal Supremo de 18 de junio de 2006 señala en su Fundamento de Derecho cuarto que:

"De lo antes expuesto resulta, falta de contradicción entre una y otra sentencia; a estos efectos debe indicarse, que en doctrina de la Sala en despido disciplinarios, como pone de relieve la parte impugnante del recurso, que la calificación de conductas, a efectos de su inclusión en el artículo 54 del ET, no es materia propia de la unificación de doctrina, ante la dificultad de que se produzcan situaciones sustancialmente iguales, ya que en estos casos, la decisión judicial, se funda en una valoración individualizada de circunstancias variables, que normalmente no permite generalizaciones de las decisiones fuera de su ámbito específico. Pues bien, de acuerdo con lo anterior, en el caso de autos, como resulta de los hechos probados, antes relacionados existe la falta de identidad sustancial entre los hechos de una y otra sentencia pues las conductas imputadas, en cada caso, pese a la aparente similitud, difieren, por lo siguiente: mientras que en la recurrida, se trataba de un trabajador que utilizó el acceso a Internet y del correo electrónico instalado por la empresa, para uso privado, entendiéndose la sentencia impugnada que estaba autorizado por la empresa, lo que deducía de la falta de prohibición específica, así como de los medios entregados al trabajador, con lo cual tenía posibilidad de mantener un ámbito privado y particular para hacer las comunicaciones con otras personas, imputadas, por lo que la investigación practicada incidía en el derecho fundamental, al inmiscuirse en el artículo 18 CE, siendo ilícita la prueba practicada causa de la improcedencia del despido, careciendo de relevancia el resto de las faltas imputadas, a los efectos del despido, en la referencial, en donde también como hechos dicho, se imputaba a un trabajador, el uso privado del acceso a Internet, y del ordenador, en horario de trabajo la causa de la decisión, estimando el despido procedente, no era la ya expuesta, en el supuesto de la sentencia recurrida, esto es entender que existió autorización del empresario, sino otra distinta, como era la transgresión de la buena fe contractual y abuso de confianza, que suponía el tiempo dedicado a la navegación por Internet superior a la hora y media por día de trabajo, sin relación con este último, considerando por tanto válida la prueba utilizada; con independencia de ello, en la referencial la práctica de la prueba para comprobar el acceso a direcciones particulares, que no debían efectuarse por ser ajenas a las propias del cometido profesional del trabajador, se hicieron en presencia de la representación unitaria, lo que da más garantía de veracidad a su resultado, lo que no acaeció en la recurrida, siendo un dato de gran relevancia a los efectos de contradicción, lo que unido al hecho de que en la recurrida se considerara que existió autorización del empresario para el uso privado de Internet, lo que no concurre en la referencial refuerza la conclusión a la que aquí llegamos."

De todo ello se desprende que la aplicación del artículo 20.3 ET no legitima por sí solo el tratamiento de las imágenes, si bien este será posible, aún sin contar con el consentimiento del afectado en caso de que el trabajador haya sido debidamente informado de la existencia de esta medida, debiendo además ser claro que, conforme a lo exigido por el artículo 4.2 LOPD, los datos no podrán ser utilizados para fines distintos.

■ CONCLUSIONES

- El tratamiento de datos de imágenes por las empresas de seguridad privada se encuentra habilitado el artículo 6.1 de la LOPD en conexión con el artículo 5.1 de la LSP, siempre que la empresa de seguridad se halle debidamente inscrita y el contrato haya sido objeto de la pertinente notificación prevista en el artículo 6.1 de la LSP o se encuentre en una de las excepciones previstas en el artículo 20 RSP.
- Los tratamientos de imágenes efectuados en entidades de crédito se encuentran amparados por el artículo 6.1 de la LOPD en conexión con el artículo 13.1 de la LOSE y el artículo 120.1 a) del RSP.
- Los tratamientos efectuados en locales, comunidades o establecimientos se encontrarán amparados por los artículos 6.1 de la LOPS y 13.1 de la LOSE si existe una decisión de los órganos competentes del Ministerio del Interior en este sentido, bien por referencia a la medida específica de videovigilancia, bien por ordenarse la creación de un departamento de seguridad (artículo 112.1 RSC).
- El tratamiento efectuado por el empresario en relación con imágenes de los trabajadores en el lugar de trabajo se encontrará habilitado por el artículo 6.2 de la LOPD siempre que el empleado haya sido debidamente informado de la medida de control adoptada conforme al artículo 20-3 ET.
- En los restantes supuestos no existe habilitación específica para el tratamiento, debiendo contarse con el consentimiento del afectado.

CONSULTAS PLANTEADAS EN 2006 SOBRE ESTA MATERIA

Dado que la Instrucción se publicó a finales del 2006, son pocas las consultas planteadas en 2006 en las que ésta resulta de aplicación. No obstante, existen consultas relacionadas con la legitimación para el tratamiento, lo demuestran los informes 0262/2006, 0298/2006, 0533/2006.

Otras cuestiones que se han planteado se refieren a si la simple reproducción de imágenes en tiempo real generan un fichero con la consiguiente obligación a inscripción. En los informes 0258/2006, 0503/2006, se aborda la cuestión y como establece el artículo 7 de la Instrucción la reproducción de imágenes en tiempo real no genera ningún fichero, si bien ello no exime de cumplir con el deber de informar que ha de darse en todo caso, por imperativo legal del artículo 5 de la LOPD.

También se ha planteado si las cámaras han de ser identificadas con algún tipo de señalización concreta. En el informe 0503/2006 se ponía de manifiesto que desde el ámbito competencial de la Agencia Española de Protección de Datos, sólo corresponde exigir el cumplimiento del deber de información, previsto en el artículo 5 LOPD, que no se

refiere a la necesidad de identificar la ubicación de las cámaras. Asimismo se indicó que respecto de la ubicación del cartel informativo, no es necesario que se coloque debajo de la cámara, siendo suficiente conforme a lo dispuesto en el artículo 3 a) de la citada Instrucción, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados. Por último, el cartel informativo debería asemejarse todo lo posible al que se encuentra disponible en la página web de la Agencia Española de Protección de Datos, con la finalidad que los ciudadanos puedan identificar fácilmente el cartel, con la existencia de una zona videovigilada y el tratamiento de sus datos para de esta manera garantizar una mayor seguridad en el conocimiento de sus derechos.

ÍNDICE

III. CÓDIGOS TIPO

III. CÓDIGOS TIPO

La elaboración de Códigos Tipo está regulada en el artículo 32 de la LOPD, que establece lo siguiente:

- “1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados e inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas”.

La AEPD considera que la autorregulación es un mecanismo de gran utilidad para desarrollar el marco de la normativa de protección de datos en determinados sectores de actividad, y en ese objetivo desde la Agencia se ha promovido la elaboración de Códigos Tipo apoyando a los sectores interesados en ello, o que se han dirigido a la Agencia.

La experiencia de la Agencia en esta materia ha puesto de manifiesto que la elaboración y aprobación de un Código Tipo no es un trámite sencillo y requiere de un análisis específico en cada uno de los casos, por lo que cualquier proyecto de Código Tipo siempre está precedido de reuniones y tomas de contacto entre los promotores del Código y de la Agencia.

Uno de los principales mensajes que desde la Agencia se ha transmitido en numerosas reuniones y sesiones de trabajo es que la decisión de adopción del código, sea que involucre a una entidad o una agrupación, en todo caso, responderá a la necesidad de ofrecer al afectado unas garantías mejoradas de la normativa general.

Por otro lado, los códigos tipo deberán incluir los principios específicos de los tratamientos de datos en los sectores o actividades a los que afecten, que mejoren las previsiones legales. Asimismo, deberán contener un resumen de ventajas y/o garantías que ofrece el código a los titulares de los datos, las obligaciones que tienen los responsables de los ficheros y los modelos para el ejercicio de los derechos reconocidos por la LOPD, sin que, en ningún caso, puedan sustituir a los mecanismos previstos en la Ley para tutelar los derechos de los afectados.

Durante el año 2006, se han presentado formalmente dos solicitudes de inscripción de Códigos tipo. La primera del "Código Tipo de Protección de datos personales del FICHERO VERAZ-PERSUS", y la segunda del CÓDIGO TIPO DE TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL PARA SERVICIOS DE PREVENCIÓN DE RIESGOS LABORALES AJENOS". Asimismo, se ha presentado formalmente solicitud de modificación de inscripción del "Código Tipo de TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ODONTÓLOGOS Y ESTOMATÓLOGOS DE ESPAÑA".

Además, se han mantenido contactos informales con representantes de empresas y asociaciones, interesadas también en la inscripción de sus respectivos Códigos Tipo, que han sido objeto de estudio por parte del RGPD. Entre ellos destacan: AMAT (ASOCIACIÓN DE MUTUAS DE ACCIDENTES DE TRABAJO Y ENFERMEDADES PROFESIONALES DE LA SEGURIDAD SOCIAL), INSTITUTO TECNOLÓGICO HOTELERO, Código Tipo APCAS y ALIAD -FEDERACIÓN NACIONAL DE CLINICAS PRIVADAS.

A continuación se exponen los principales aspectos de los diferentes Proyectos que han sido objeto de estudio y evaluación durante 2006:

■ CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES DEL FICHERO VERAZ-PERSUS

Este Código Tipo se inscribió en el RGPD, con fecha 21 de diciembre de 2006, con el número de expediente CT/0001/2006, y ha sido promovido por Soluciones Veraz Asnef-Equifax, S.L.

Con este Código Tipo se pretende alcanzar una doble finalidad: garantizar el adecuado y leal tratamiento de los datos de carácter personal de los interesados en el fichero VERAZ-PERSUS, en consonancia con la legislación vigente en materia de protección de datos, así como la protección a los intereses de los ciudadanos y consumidores, asentados en los principios de transparencia y flexibilidad.

El fichero VERAZ-PERSUS tiene como objetivo el prevenir conductas perjudiciales para el mercado y para los ciudadanos. En este sentido, las personas que deseen proteger su patrimonio económico voluntariamente pueden solicitar su auto-inclusión a este fichero para prevenir eventuales estafas por suplantación de su personalidad.

Con el mismo objetivo, el fichero otorga amparo a las personas que se encuentran en cualquier situación legal de incapacidad y a menores, a través de sus tutores legales,

siempre con el máximo respeto a la intimidad de dichas personas y a su situación de incapacidad; garantizando la adecuada confidencialidad de la causa de la incapacidad legal en la que se encuentren las personas que puedan autoincluirse a través de sus tutores legales en el fichero VERAZ-PERSUS, garantizando que en ningún caso se tratarán datos especialmente protegidos, de los establecidos en los artículos 7 y 8 de la LOPD.

Dada la innovación que supone la creación de un fichero de estas características, con el fin de sentar las bases de actuación en el ámbito de la autorregulación, el Código Tipo pretende obtener las garantías necesarias en el respeto a los principios y disposiciones de la legislación vigente en materia de protección de datos personales.

La presentación del Código Tipo del fichero VERAZ-PERSUS persigue establecer un procedimiento de conducta de obligado cumplimiento para las entidades usuarias, coordinando la actuación de las mismas en la protección de los datos personales de los interesados; facilitar y agilizar el ejercicio de los derechos de carácter personal; y adoptar un marco de publicidad necesaria, dada la novedosa forma planteada en el ámbito de la defensa contra las conductas atentatorias al patrimonio económico de los consumidores y ciudadanos, disminuyendo, la aparición de factores de inquietud social.

Las entidades que podrán adherirse al Código Tipo son cualquier empresa u organismo público o privado, que estén autorizadas y ejerzan legalmente en España, en cualquiera de sus modalidades, en relación con la realización de operaciones crediticias de cualquier modalidad, de financiación mediante pago aplazado de bienes muebles, ya sean de consumo duradero o de equipo y emisores de tarjetas de crédito. También podrán adherirse empresas de servicios -agua, luz, gas, teléfono- y entidades que colaboran en la lucha contra el fraude, así como cualquier ente u organismo público que participe en la consecución de los objetivos y finalidades del presente Código Tipo.

En relación con el derecho de autoinclusión, cualquier persona, por sí misma o a través de su tutor legal, podrá solicitar la inclusión de sus datos personales en el fichero VERAZ-PERSUS con el fin de proteger su identidad, solvencia y/o evitar que sus bienes económicos pudieran verse afectados por el extravío o robo de su documentación o por la concurrencia de estafa por suplantación de su personalidad. Dicha solicitud es voluntaria y podrá ser revocable en cualquier momento.

Para la inclusión por parte del propio interesado deben presentar: el modelo de autoinclusión debidamente cumplimentado y firmado, una fotocopia del documento nacional de identidad, tarjeta de residencia, pasaporte o cualquier documento acreditativo de su identidad, y una fotocopia de la denuncia interpuesta en una Comisaría de Policía o Puestos de la Guardia Civil que acredite la ausencia de dicha documentación.

■ CÓDIGO TIPO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ODONTÓLOGOS Y ESTOMATÓLOGOS DE ESPAÑA

Este Código Tipo de tratamiento de datos de carácter personal para Odontólogos y Estomatólogos de España, se inscribió en el RGPD, mediante resolución de 6 de julio

de 2004, del Director de la Agencia Española de Protección de Datos, con el número de expediente CT/0002/2004. En el año 2006, solicitaron una modificación del mismo, la cual concluyó el 22 de diciembre de 2006, fecha en que se procedió a su inscripción en el RGPD.

El motivo alegado para solicitar la inscripción del texto modificado es, que la Asamblea General del Ilustre Consejo General de Colegios Oficiales de Odontólogos y Estomatólogos de España, en su reunión celebrada el día 15 de diciembre de 2006, acordó por unanimidad modificar el apartado c) del artículo 16 del "Código Tipo de tratamiento de datos de carácter personal para Odontólogos y Estomatólogos de España", a los efectos de suprimir la expresión "En concreto, el nombre, apellidos, fecha de nacimiento y el tratamiento a realizar", y sustituirla por la siguiente "y, en concreto, el nombre y apellidos o un código de referencia que permita, en su caso, la trazabilidad de la prótesis".

La razón principal por la que la Asamblea General acordó la modificación señalada, es la de considerar que los datos objeto de supresión no son relevantes ni necesarios para la actuación profesional a desarrollar por los protésicos dentales, entre otros, por los siguientes motivos:

- En relación con el nombre y los apellidos de los pacientes, aunque se trate de datos requeridos por el Real Decreto 414/1996, que traspone la Directiva Comunitaria 93/42/CEE, de 14 de junio de 1993, los mismos pueden ser sustituidos por un código facultativo que permita conservar la "trazabilidad" del producto sanitario, tal y como ha manifestado la Comisión Europea en respuesta a la consulta del eurodiputado Sr. Nencini, publicado en el Diario de las Comunidades Europeas de 9 de octubre de 1998. Asimismo, el Tribunal Supremo, en sentencia de fecha 21 de diciembre de 1998, reconoce la posibilidad, al amparo del deber de confidencialidad, de silenciar el nombre de los pacientes, al señalar, expresamente que:
- "...con independencia de que proporcionar datos identificadores del paciente pueda afectar a la intimidad de éste y formar parte del secreto médico, resulta indiscutible que su inclusión entre las indicaciones que debe realizar el facultativo al protésico no es una obligación legal, no está impuesta por la ley que desarrolla el real Decreto o por otro precepto legal de igual rango, ni los referidos datos resultan imprescindibles para el trabajo o actividad profesional del protésico".
- Por lo tanto, no es absolutamente imprescindible que las Clínicas comuniquen a los protésicos dentales el nombre y apellidos de sus pacientes, si bien en este supuesto las Clínicas deberán instaurar un sistema de identificación inmediata de los pacientes mediante códigos para eventuales necesidades de trazabilidad de productos o materiales defectuosos o peligrosos para la salud.
- Por otra parte, se ha modificado en todo el texto del código el término "paciente o usuario" por "paciente o usuario de los servicios de salud bucodental" así como el término "auditoria bianual" por "auditoria bienal".

Y por último, en el procedimiento de adhesión al Código, se ha ampliado a tres meses el plazo del que dispone el Órgano de Control del Código Tipo para dictar una resolución expresa acerca de la aceptación o denegación de adhesión al Código Tipo.

■ **CÓDIGO TIPO DE TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL PARA SERVICIOS DE PREVENCIÓN DE RIESGOS LABORALES AJENOS**

En el mes de noviembre de 2006, fue presentada al RGPD una solicitud de inscripción por parte de la FEDERACIÓN DE SERVICIOS DE PREVENCIÓN AJENOS, del CÓDIGO TIPO DE TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL PARA SERVICIOS DE PREVENCIÓN DE RIESGOS LABORALES AJENOS.

Este proyecto de código pretende sensibilizar al sector de la Prevención de Riesgos Laborales, sobre la importancia de la protección de los datos personales y especialmente sobre la obligatoriedad de tratar los mismos con absoluta confidencialidad.

Tras el estudio y revisión del proyecto presentado, el RGPD observó determinados aspectos que deberían ser modificados para adecuarse a lo exigido en el artículo 32 de la LOPD, por lo se efectuó el correspondiente requerimiento.

En la fecha en que se ha confeccionado la presente memoria de 2006, se significa que se ha archivado por desistimiento el citado expediente, pero que la FEDERACIÓN DE SERVICIOS DE PREVENCIÓN AJENOS continúa con la elaboración del código.

Cifras

2006

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



INDICE

175 REGISTRO GENERAL DE PROTECCIÓN DE DATOS

- 176 EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD
- 176 FICHEROS INSCRITOS
- 176 INCREMENTO ANUAL
- 177 DATOS RELACIONADOS CON LA INSCRIPCIÓN EN 2006
- 177 OPERACIONES DE INSCRIPCIÓN
- 178 DATOS RELACIONADOS CON LA INSCRIPCIÓN DURANTE 2006
- 178 DISTRIBUCIÓN DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD
- 179 RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD
- 179 DOCUMENTOS DE ENTRADA SEGÚN EL TIPO DE SOPORTE DE LA NOTIFICACIÓN
- 180 INSCRIPCIÓN DE TITULARIDAD PRIVADA
- 180 DISTRIBUCIÓN DE FICHEROS
- 182 DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS
- 182 DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES
- 183 DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD
- 184 DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS
- 184 FICHEROS CON CESIONES DE DATOS
- 185 DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD
- 186 INSCRIPCIÓN DE TITULARIDAD PÚBLICA
- 186 FICHEROS INSCRITOS: INCREMENTO ANUAL
- 186 DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN
- 187 DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL
- 187 DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS
- 188 DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL
- 190 DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS
- 190 DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS
- 191 DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES
- 192 DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD
- 193 DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS
- 193 FICHEROS CON CESIONES DE DATOS
- 194 TRANSFERENCIAS INTERNACIONALES DE DATOS
- 194 RESOLUCIONES DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES A TERCEROS PAÍSES CON NIVEL DE PROTECCIÓN NO ADECUADO
- 195 FICHEROS INSCRITOS QUE DECLARAN TRANSFERENCIAS INTERNACIONALES
- 196 DERECHO DE CONSULTA AL REGISTRO
- 196 DATOS SOBRE CONSULTAS AL APARTADO FICHEROS INSCRITOS EN LA WEB
- 197 ACCESOS AL CANAL DEL RESPONSABLE EN LA WEB

199 SUBDIRECCIÓN GENERAL DE INSPECCIÓN

- 200 ESTADÍSTICAS RELATIVAS AL REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN
- 200 REGISTRO DE DOCUMENTACIÓN
- 201 ESTADÍSTICAS RELATIVAS A ACTUACIONES Y PROCEDIMIENTOS INICIADOS Y FINALIZADOS
- 201 ACTUACIONES Y PROCEDIMIENTOS INICIADOS (ÁREA DE INSPECCIÓN)
- 201 ACTUACIONES Y PROCEDIMIENTOS FINALIZADOS (ÁREA DE INSTRUCCIÓN)
- 202 ACTUACIONES PREVIAS DE INVESTIGACIÓN
- 202 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO
- 203 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL DENUNCIANTE
- 203 ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL INVESTIGADO
- 204 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO
- 205 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR FINANCIERO
- 205 ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR TELECOMUNICACIONES
- 206 ACTUACIONES POSTERIORES A LA INSPECCIÓN
- 206 RESOLUCIONES DE ARCHIVO
- 207 PROCEDIMIENTOS SANCIONADORES INICIADOS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO
- 208 PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO
- 209 PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006 POR SECTOR DE ACTIVIDAD DEL PRINCIPAL IMPUTADO
- 210 PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR COMUNIDAD AUTÓNOMA EN LA QUE RADICA LA ADMINISTRACIÓN IMPUTADA
- 211 PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR TIPO DE ADMINISTRACIÓN
- 211 PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS FINALIZADOS POR TIPO DE ADMINISTRACIÓN
- 212 TUTELAS DE DERECHOS
- 212 PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR DERECHO TUTELADO
- 212 PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR COMUNIDAD AUTÓNOMA DEL RECLAMANTE
- 213 RECURSOS DE REPOSICIÓN

215 SECRETARÍA GENERAL

216 RECURSOS HUMANOS

- 216 EFECTIVOS DE LA AGPD POR SEXO
- 216 RELACIÓN DE EFECTIVOS POR GRUPOS
- 217 RELACIÓN DE EFECTIVOS POR NIVELES

218 ÁREA DE ATENCIÓN AL CIUDADANO

- 218 CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO
- 218 COMPARACIÓN CON AÑOS ANTERIORES
- 219 EVOLUCIÓN DE LAS CONSULTAS PLANTEADAS A TRAVÉS DE INTERNET
- 219 ANÁLISIS DE LAS CONSULTAS POR TEMAS 2006
- 220 EXAMEN DEL APARTADO SOBRE DERECHOS 2006
- 221 ACCESOS A LA PÁGINA WEB AÑO 2006
- 221 EVOLUCIÓN GRÁFICA DE LOS ACCESOS WEB DURANTE EL AÑO 2006
- 222 COMPARATIVA ACCESOS WEB 2005-2006
- 223 REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006. COMPARATIVA CON AÑOS ANTERIORES
- 224 REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006 EN EL ÁREA DE ADMINISTRACIÓN GENERAL Y ATENCIÓN AL CIUDADANO. COMPARATIVA CON AÑOS ANTERIORES

225 GESTIÓN ECONÓMICA

- 225 PRESUPUESTO DE INGRESOS
- 225 ANÁLISIS CAPÍTULO MULTAS Y SANCIONES SOBRE DERECHOS RECONOCIDOS
- 226 PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULO
- 227 PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULO. OBLIGACIONES RECONOCIDAS
- 228 EJECUCIÓN PRESUPUESTARIA 2002
- 228 EJECUCIÓN PRESUPUESTARIA 2003
- 229 EJECUCIÓN PRESUPUESTARIA 2004
- 229 EJECUCIÓN PRESUPUESTARIA 2005
- 230 EJECUCIÓN PRESUPUESTARIA 2006
- 231 COMPOSICIÓN DEL INMOVILIZADO A 31 DICIEMBRE 2006
- 231 DETALLE DEL INMOVILIZADO A 31 DICIEMBRE 2006

233 AREA INTERNACIONAL

- 235 ASISTENCIA A REUNIONES EN EL ÁMBITO INTERNACIONAL DURANTE EL AÑO 2006

237 GABINETE JURÍDICO

238 INFORMES PRECEPTIVOS

- 238 EVOLUCIÓN DE INFORMES Y DISPOSICIONES
- 239 EVOLUCIÓN DE INFORMES PRECEPTIVOS

240 CONSULTAS PLANTEADAS

- 240 EVOLUCIÓN DE CONSULTAS 2002-2006
- 240 DISTRIBUCIÓN DE CONSULTAS 2006
- 241 DISTRIBUCIÓN DE CONSULTAS SECTOR PÚBLICO- SECTOR PRIVADO
- 242 CONSULTAS PLANTEADAS: DISTRIBUCIÓN SECTORIAL
- 242 DISTRIBUCIÓN DE LAS CONSULTAS POR SECTORES
- 243 EVOLUCIÓN CONSULTAS POR SECTORES (2005-2006)

244 CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

- 244 CONSULTAS POR MATERIAS
- 245 EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS (2005-2006)
- 246 CONSULTAS SOBRE CESIONES DE DATOS
- 247 CONSULTAS POR COMUNIDADES AUTÓNOMAS
- 248 CONSULTAS POR PROVINCIAS

249 SENTENCIAS: ÓRGANOS ENJUICIADORES

- 249 SENTENCIAS POR ÓRGANO JURISDICCIONAL

250 SENTENCIAS: SENTIDO DEL FALLO

- 250 SENTENCIAS DE LA AUDIENCIA NACIONAL
- 250 COMPARATIVA SENTENCIAS EN PRIMERA O ÚNICA INSTANCIA (PORCENTAJES)

251 SENTENCIAS: DISTRIBUCIÓN SECTORIAL

- 251 SENTENCIAS POR SECTORES
- 251 COMPARATIVA POR SECTORES

252 SENTENCIAS: DISTRIBUCIÓN POR MATERIAS

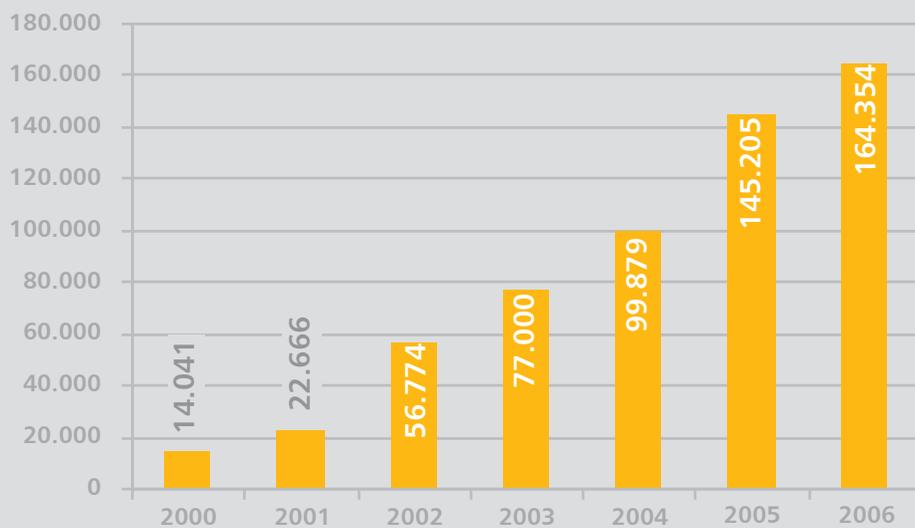
- 252 SENTENCIAS POR MATERIAS
- 253 COMPARATIVA DE SENTENCIAS POR MATERIAS (2003-2006)
- 254 SENTENCIAS SOBRE FICHEROS DE SOLVENCIA PATRIMONIAL
- 254 RESOLUCIONES EN CASACIÓN

EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD

FICHEROS INSCRITOS

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
TITULARIDAD PÚBLICA	20.198	24.923	26.541	27.969	28.890	30.431	31.155	31.805	35.894	43.974	48.038	51.817	56.138
TITULARIDAD PRIVADA	192.097	199.933	201.054	201.835	203.138	204.737	218.054	240.070	292.755	361.675	457.490	598.916	758.955
TOTALES	212.295	224.856	227.595	229.804	232.028	235.168	249.209	271.875	328.649	405.649	505.528	650.733	815.093

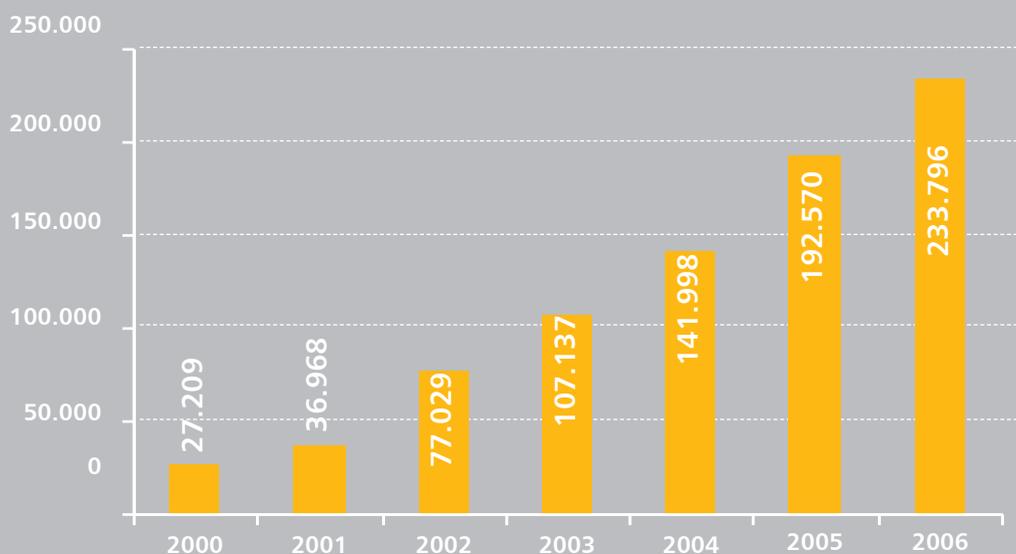
INCREMENTO ANUAL



EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD

DATOS RELACIONADOS CON LA INSCRIPCIÓN EN 2006

	2005	2006	INCREMENTO	MEDIA DIARIA EN 2005	MEDIA DIARIA EN 2006
OPERACIONES DE INSCRIPCIÓN	192.570	233.796	21%	802	974
DOCUMENTOS DE ENTRADA	99.837	110.259	10%	416	459
DOCUMENTOS DE SALIDA	191.392	215.170	12%	797	897
NOTIFICACIONES DE RESOLUCIÓN DEL DIRECTOR	179.834	203.769	13%	749	849
TOTAL DE FICHEROS INSCRITOS	650.733	815.093	25%	605	685

OPERACIONES DE INSCRIPCIÓN¹

¹ Este gráfico muestra la evolución de las operaciones de inscripción en el Registro General de Protección de Datos desde la entrada en vigor de la LOPD.

DATOS RELACIONADOS CON LA INSCRIPCIÓN DURANTE 2006

DISTRIBUCIÓN DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD²

REGISTROS DE ENTRADA

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
NOTIFICACIONES													
INSCRIPCIÓN	8.037	8.944	9.821	8.044	9.731	9.992	8.835	6.552	6.637	7.682	9.850	10.272	104.397
REGISTRO TELEMÁTICO	--	--	--	--	--	--	--	--	197	132	433	590	1.352
REGISTRO CONVENCIONAL	8.037	8.944	9.821	8.044	9.731	9.992	8.835	6.552	6.440	7.550	9.417	9.682	103.045
SISTEMA ANTERIOR	8.037	8.944	9.821	8.044	9.731	9.992	8.835	6.552	6.310	6.309	7.808	6.438	96.821
SOPORTE PAPEL	1.170	781	969	844	866	1.003	854	604	654	761	1.215	355	10.076
SOPORTE MAGNÉTICO	310	432	359	285	330	493	409	260	212	282	398	287	4.057
INTERNET	6.557	7.731	8.493	6.915	8.535	8.496	7.572	5.688	5.444	5.266	6.195	5.796	82.688
SISTEMA NOTA	--	--	--	--	--	--	--	--	130	1.241	1.609	3.244	6.224
SOPORTE PAPEL	--	--	--	--	--	--	--	--	10	98	322	295	725
INTERNET	--	--	--	--	--	--	--	--	120	1.143	1.287	2.949	5.499
OTRAS SOLICITUDES	542	590	638	583	517	555	715	392	456	707	681	833	7.209
TOTALES	8.579	9.534	10.459	8.627	10.248	10.547	9.550	6.944	7.093	8.389	10.531	11.105	111.606

REGISTROS DE SALIDA

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
RESOLUCIONES													
INSCRIPCIÓN (ALTAS, MODIFICACIONES Y SUPRESIONES)	14.662	16.929	18.053	15.803	18.133	18.709	16.519	15.619	12.830	14.973	16.084	25.455	203.769
REQUERIMIENTOS DEL RGPD	613	456	509	629	508	562	1.038	590	460	519	715	739	7.338
SALIDAS VARIAS ³	348	380	461	406	363	425	360	319	265	245	370	121	4.063
TOTALES	15.623	17.765	19.023	16.838	19.004	19.696	17.917	16.528	13.555	15.737	17.169	26.315	215.170

² Cada documento de entrada genera aproximadamente dos documentos de salida por término medio.³ Consultas y certificados de inscripción de ficheros, notificaciones de resoluciones de archivo, códigos tipo y otros documentos.

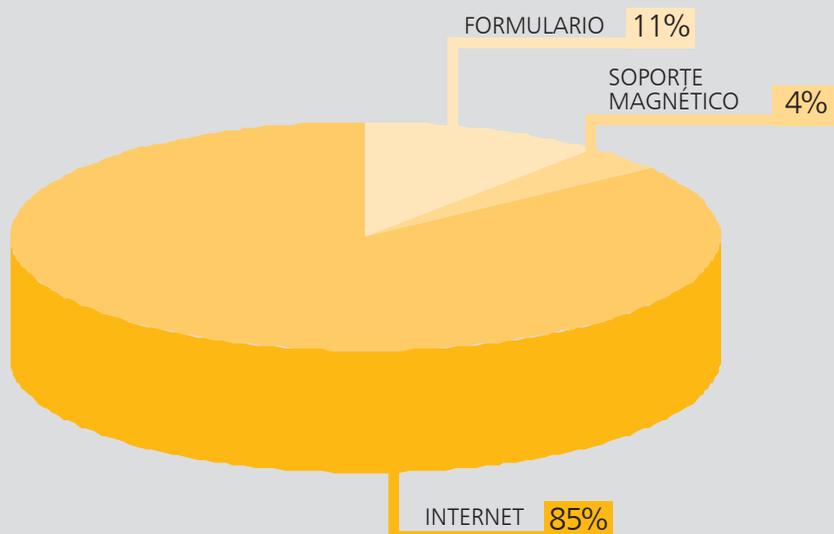
DATOS RELACIONADOS CON LA INSCRIPCIÓN DURANTE 2006

RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD

OPERACIONES DE INSCRIPCIÓN

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
ALTAS	12.704	14.309	15.864	13.285	15.692	16.275	14.891	13.177	10.580	12.699	13.850	23.266	176.592
MODIFICACIONES	1.130	1.363	1.308	1.461	1.232	1.513	1.188	1.282	735	1.150	1.336	1.248	14.946
SUPRESIONES	828	1.257	881	1.057	1.209	921	440	1.160	1.515	1.124	898	941	12.231
SUBSANACIONES	3.564	2.385	1.398	1.116	1.590	2.557	1.070	654	1.232	1.155	1.567	11.749	30.037
TOTALES	18.226	19.314	19.451	16.919	19.723	21.266	17.589	16.273	14.062	16.128	17.651	37.204	233.806

DOCUMENTOS DE ENTRADA SEGÚN EL TIPO DE SOPORTE DE LA NOTIFICACIÓN



INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS

	RESPONSABLES		FICHEROS	
	2006	TOTAL	2006	TOTAL
COMUNIDAD AUTÓNOMA DE ANDALUCÍA	6.055	27.849	19.035	74.718
ALMERÍA	980	2.367	2.528	6.781
CÁDIZ	467	3.791	1.683	9.669
CÓRDOBA	505	2.797	2.176	8.176
GRANADA	990	3.564	3.505	11.630
HUELVA	230	1.076	1.170	2.840
JAÉN	431	1.973	1.702	6.450
MÁLAGA	1.780	7.935	3.671	16.176
SEVILLA	690	4.420	2.600	12.993
COMUNIDAD AUTÓNOMA DE ARAGÓN	2.412	15.836	5.364	31.645
HUESCA	252	3.192	688	6.050
TERUEL	50	785	196	1.576
ZARAGOZA	2.110	11.874	4.480	24.019
COMUNIDAD AUTÓNOMA DEL PRINCIPADO DE ASTURIAS	2.726	8.067	9.395	25.423
COMUNIDAD AUTÓNOMA DE CANARIAS	1.382	6.750	4.662	23.652
LAS PALMAS	639	3.457	2.477	13.603
SANTA CRUZ DE TENERIFE	745	3.316	2.185	10.049
COMUNIDAD AUTÓNOMA DE CANTABRIA	1.140	2.759	1.941	6.023
COMUNIDAD AUTÓNOMA DE CASTILLA Y LEÓN	2.363	10.931	6.233	25.439
ÁVILA	87	782	225	1.363
BURGOS	707	2.958	1.386	6.198
LEÓN	530	1.709	1.412	4.083
PALENCIA	138	598	365	1.465
SALAMANCA	203	1.092	665	2.780
SEGOVIA	81	525	269	1.110
SORIA	37	396	130	959
VALLADOLID	519	2.205	1.492	5.912
ZAMORA	67	692	289	1.569
COMUNIDAD AUTÓNOMA DE CASTILLA-LA MANCHA	1.428	6.630	4.752	19.001
ALBACETE	474	1.867	1.569	5.483
CIUDAD REAL	267	1.453	1.092	5.018
CUENCA	143	1.136	460	2.355
GUADALAJARA	170	576	517	1.601
TOLEDO	375	1.607	1.114	4.544

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS

	RESPONSABLES		FICHEROS	
	2006	TOTAL	2006	TOTAL
COMUNIDAD AUTÓNOMA DE CATALUÑA	19.923	99.182	37.428	210.150
BARCELONA	13.833	77.248	27.616	163.681
GIRONA	2.605	9.300	4.750	19.652
LLEIDA	488	5.475	1.057	11.184
TARRAGONA	2.375	7.302	4.005	15.633
COMUNIDAD DE MADRID	13.677	50.228	27.855	123.868
COMUNIDAD VALENCIANA	7.046	33.590	14.952	73.582
ALICANTE	3.132	11.064	5.690	22.151
CASTELLÓN DE LA PLANA	308	4.636	1.000	11.284
VALENCIA	3.610	17.924	8.262	40.147
COMUNIDAD AUTÓNOMA DE EXTREMADURA	929	5.272	2.388	12.552
BADAJOZ	613	3.784	1.485	8.940
CÁCERES	318	1.497	903	3.612
COMUNIDAD AUTÓNOMA DE GALICIA	4.580	19.100	15.777	53.398
A CORUÑA	1.711	8.933	5.275	23.267
LUGO	784	3.491	2.288	8.418
OURENSE	299	1.392	1.105	4.149
PONTEVEDRA	1.798	5.336	7.109	17.564
COMUNIDAD AUTÓNOMA DE LAS ILLES BALEARS	1.627	4.328	5.238	13.979
COMUNIDAD FORAL DE NAVARRA	869	4.006	2.109	9.742
COMUNIDAD AUTÓNOMA DEL PAÍS VASCO	3.185	11.461	7.300	29.597
ÁLAVA ...	400	1.882	1.084	5.049
GUIPÚZCOA	1.411	4.414	2.695	10.749
VIZCAYA	1.374	5.183	3.521	13.799
COMUNIDAD AUTÓNOMA DE LA RIOJA	593	3.493	1.955	8.175
COMUNIDAD AUTÓNOMA DE LA REGIÓN DE MURCIA	2.111	8.050	4.090	17.495
CIUDAD AUTÓNOMA DE CEUTA	8	114	31	275
CIUDAD AUTÓNOMA DE MELILLA	21	76	61	186

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS

	2006	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS (IDEOLOGÍA, CREENCIAS, RELIGIÓN Y AFILIACIÓN SINDICAL)	9.882	25.514
OTROS DATOS ESPECIALMENTE PROTEGIDOS (ORIGEN RACIAL, SALUD Y VIDA SEXUAL)	28.657	113.393
DATOS DE CARÁCTER IDENTIFICATIVO	170.573	758.955
DATOS DE CARACTERÍSTICAS PERSONALES	72.073	341.124
DATOS DE CIRCUNSTANCIAS SOCIALES	44.339	156.562
DATOS ACADÉMICOS Y PROFESIONALES	41.525	160.801
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	61.830	275.372
DATOS DE INFORMACIÓN COMERCIAL	43.864	171.076
DATOS ECONÓMICO-FINANCIEROS	119.149	475.877
DATOS DE TRANSACCIONES	61.355	250.488
OTROS TIPOS DE DATOS	173	1.229

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES

	2006	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	9.882	25.514
IDEOLOGÍA	1.746	2.686
CREENCIAS	1.642	2.546
RELIGIÓN	2.823	6.905
AFILIACIÓN SINDICAL	8.892	21.826
OTROS DATOS ESPECIALMENTE PROTEGIDOS	28.657	113.393
ORIGEN RACIAL	1.863	3.169
SALUD	28.574	113.231
VIDA SEXUAL	1.830	3.583

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD

	2006	TOTAL
GESTIÓN DE CLIENTES, CONTABLE, FISCAL Y ADMINISTRATIVA	130.917	575.774
RECURSOS HUMANOS	40.707	179.722
GESTIÓN DE NÓMINAS	34.363	112.811
PREVENCIÓN DE RIESGOS LABORALES	12.268	35.721
SERVICIOS ECONÓMICO-FINANCIEROS Y SEGUROS	8.336	47.019
CUMPLIMIENTO/INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS	9.279	22.952
PRESTACIÓN DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CRÉDITO	527	4.655
PUBLICIDAD Y PROSPECCIÓN COMERCIAL	13.934	74.734
ANÁLISIS DE PERFILES	1.487	6.937
PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES	596	3.713
GUÍAS/REPERTORIOS DE SERVICIOS DE TELECOMUNICACIONES	175	809
COMERCIO ELECTRÓNICO	1.039	4.324
PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN	284	664
GESTIÓN DE ASOCIADOS O MIEMBROS DE PARTIDOS POLÍTICOS, SINDICATOS, IGLESIAS, CONFESIONES O COMUNIDADES RELIGIOSAS Y ASOCIACIONES, FUNDACIONES Y OTRAS ENTIDADES SIN ÁNIMO DE LUCRO	1.027	4.025
ACTIVIDADES ASOCIATIVAS DIVERSAS	5.808	22.333
ASISTENCIA SOCIAL	721	2.428
EDUCACIÓN	3.039	13.800
GESTIÓN Y CONTROL SANITARIO	5.442	42.583
HISTORIAL CLÍNICO	4.346	29.439
INVESTIGACIÓN EPIDEMIOLOGICA Y ACTIVIDADES ANÁLOGAS	537	5.702
VIDEOVIGILANCIA	41	41
SEGURIDAD Y CONTROL ACCESO A EDIFICIOS	1.686	5.443
SEGURIDAD PRIVADA	1.564	4.784
FINES HISTÓRICOS, CIENTÍFICOS O ESTADÍSTICOS	4.472	66.715
OTRAS FINALIDADES	20.889	92.845

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS

	2006	TOTAL
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	169.159	731.983
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	12.279	44.825
FUENTES ACCESIBLES AL PÚBLICO	10.186	37.126
REGISTROS PÚBLICOS	9.657	27.808
ENTIDAD PRIVADA	11.801	57.942
ADMINISTRACIONES PÚBLICAS	7.093	21.655

FICHEROS CON CESIONES DE DATOS

INSCRITOS EN 2006	TOTAL
44.957	143.409

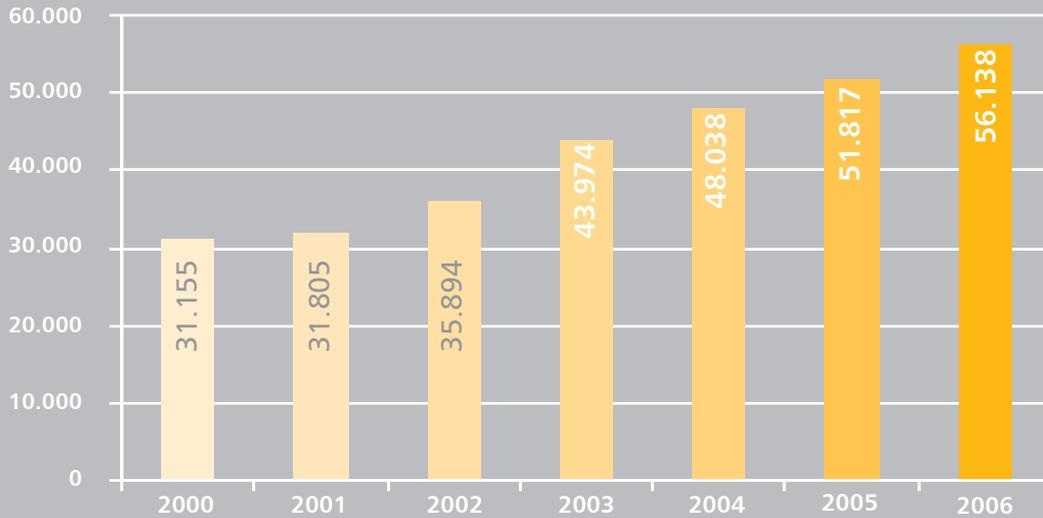
INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD

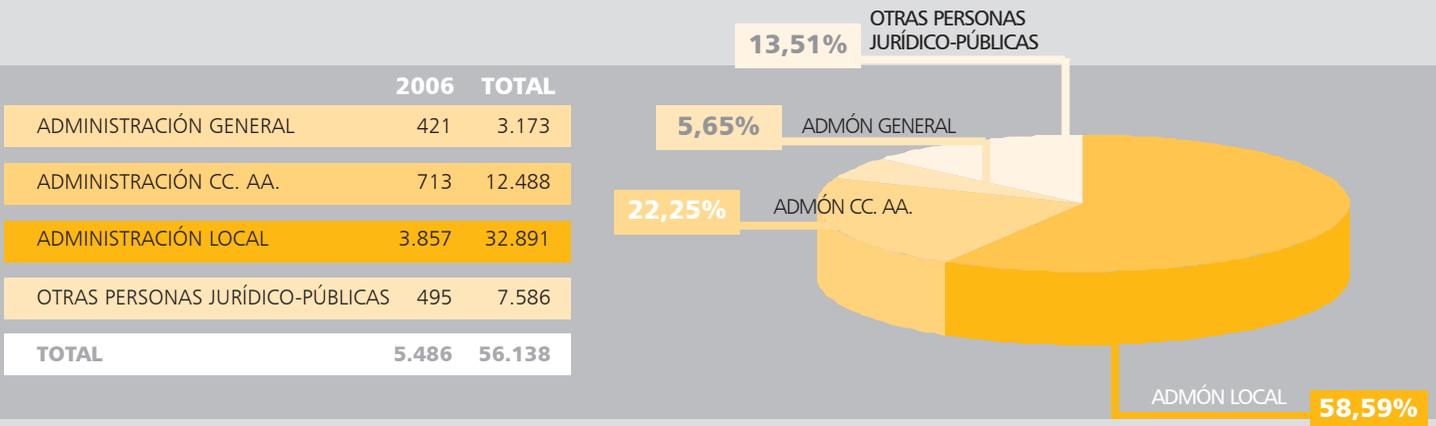
DESCRIPCIÓN DE LA ACTIVIDAD PRINCIPAL	2006	TOTAL
COMUNIDADES DE PROPIETARIOS	30.971	68.068
ACTIVIDADES JURÍDICAS, NOTARIOS Y REGISTRADORES	15.555	22.739
COMERCIO	12.053	95.141
ACTIVIDADES INMOBILIARIAS	11.155	40.365
CONTABILIDAD, AUDITORÍA Y ASESORÍA FISCAL	10.664	57.491
SANIDAD	9.323	56.816
ASOCIACIONES Y CLUBES	7.696	22.618
CONSTRUCCIÓN	6.009	29.137
EDUCACIÓN	4.536	19.264
TURISMO Y HOSTELERÍA	4.369	26.493
INDUSTRIA QUÍMICA Y FARMACÉUTICA	3.889	27.550
SERVICIOS INFORMÁTICOS	3.210	15.383
MAQUINARIA Y MEDIOS DE TRANSPORTE	2.758	19.898
SEGUROS PRIVADOS	2.389	14.535
TRANSPORTE	2.378	15.783
ACTIVIDADES DE SERVICIOS SOCIALES	1.802	6.359
ACTIVIDADES RELACIONADAS CON LOS PRODUCTOS ALIMENTICIOS, BEBIDAS Y TABACOS	1.726	13.530
SECTOR ENERGÉTICO	1.559	9.031
AGRICULTURA, GANADERÍA, EXPLOTACIÓN FORESTAL, CAZA Y PESCA	1.492	11.504
ACTIVIDADES DIVERSAS DE SERVICIOS PERSONALES	1.401	7.100
ENTIDADES BANCARIAS Y FINANCIERAS	1.400	11.097
PRODUCCIÓN DE BIENES DE CONSUMO	1.053	9.997
PUBLICIDAD DIRECTA	926	5.222
ACTIVIDADES DE ORGANIZACIONES EMPRESARIALES, PROFESIONALES Y PATRONALES	800	6.000
SERVICIOS DE TELECOMUNICACIONES	785	4.320
SELECCIÓN DE PERSONAL	577	2.400
ACTIVIDADES RELACIONADAS CON LOS JUEGOS DE AZAR Y APUESTAS	540	2.943
SEGURIDAD	459	2.457
INVESTIGACIÓN Y DESARROLLO (I+D)	282	1.646
ORGANIZACIÓN DE FERIAS, EXHIBICIONES, CONGRESOS Y OTRAS ACTIVIDADES RELACIONADAS	212	770
ACTIVIDADES POLÍTICAS, SINDICALES Y RELIGIOSAS	210	1.415
INSPECCIÓN TÉCNICA DE VEHÍCULOS Y OTROS ANÁLISIS TÉCNICOS	90	532
ACTIVIDADES POSTALES Y DE CORREO (OPERADORES POSTALES, EMPRESAS PRESTADORAS DE SERVICIOS POSTALES, TRANSPORTISTAS Y EMPRESAS DE ACTIVIDADES AUXILIARES Y COMPLEMENTARIAS DEL TRANSPORTE)	89	1.730
SOLVENCIA PATRIMONIAL Y CRÉDITO	79	598
MUTUALIDADES COLABORADORAS DE LOS ORGANISMOS DE LA SEGURIDAD SOCIAL	76	792
COMERCIO Y SERVICIOS ELECTRÓNICOS	62	63
OTRAS ACTIVIDADES	25.476	91.407

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

FICHEROS INSCRITOS: INCREMENTO ANUAL



DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN



INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

A los efectos de esta distribución, se consideran integrados en Administración General, a la Administración General del Estado, Entidades y Organismos de la Seguridad Social y Organismos Autónomos del Estado.

PRESIDENCIA DEL GOBIERNO	6
MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN	522
MINISTERIO DE JUSTICIA	35
MINISTERIO DE DEFENSA	48
MINISTERIO DE ECONOMÍA Y HACIENDA	273
MINISTERIO DEL INTERIOR	176
MINISTERIO DE FOMENTO	202
MINISTERIO DE EDUCACIÓN Y CIENCIA	196
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	808
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIÓN	64
MINISTERIO DE LA PRESIDENCIA	56
MINISTERIO DE ADMINISTRACIONES PÚBLICAS	219
MINISTERIO DE SANIDAD Y CONSUMO	112
MINISTERIO DE MEDIO AMBIENTE	194
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO	170
MINISTERIO DE CULTURA	82
MINISTERIO DE VIVIENDA	10
TOTAL	3.173

DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS

Aparecen aquí los ficheros de la Administración de Comunidades Autónomas, así como los de los Organismos Públicos dependientes de éstas

	2006	TOTAL
COMUNIDAD AUTÓNOMA DE ANDALUCÍA	145	1.363
COMUNIDAD AUTÓNOMA DE ARAGÓN	--	237
COMUNIDAD AUTÓNOMA DEL PRINCIPADO DE ASTURIAS	11	241
COMUNIDAD AUTÓNOMA DE CANARIAS	15	397
COMUNIDAD AUTÓNOMA DE CANTABRIA	6	57
COMUNIDAD AUTÓNOMA DE CASTILLA Y LEÓN	96	467
COMUNIDAD AUTÓNOMA DE CASTILLA-LA MANCHA	137	363
COMUNIDAD AUTÓNOMA DE CATALUÑA	111	581
COMUNIDAD DE MADRID	28	6.066
COMUNIDAD VALENCIANA	45	554
COMUNIDAD AUTÓNOMA DE EXTREMADURA	17	163
COMUNIDAD AUTÓNOMA DE GALICIA	26	768
COMUNIDAD AUTÓNOMA DE LAS ILLES BALEARS	9	72
COMUNIDAD FORAL DE NAVARRA	9	125
COMUNIDAD AUTÓNOMA DEL PAÍS VASCO	13	458
COMUNIDAD AUTÓNOMA DE LA RIOJA	19	187
COMUNIDAD AUTÓNOMA DE LA REGIÓN DE MURCIA	26	304
CIUDAD AUTÓNOMA DE CEUTA	--	23
CIUDAD AUTÓNOMA DE MELILLA	--	62
TOTAL	713	12.488

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
COMUNIDAD AUTÓNOMA DE ANDALUCÍA	715	6.260
ALMERÍA	104	951
CÁDIZ	45	527
CÓRDOBA	71	546
GRANADA	170	1.277
HUELVA	85	1.170
JAÉN	85	523
MÁLAGA	53	438
SEVILLA	102	828
COMUNIDAD AUTÓNOMA DE ARAGÓN	468	2.966
HUESCA	159	598
TERUEL	47	171
ZARAGOZA	262	2.197
COMUNIDAD AUTÓNOMA DEL PRINCIPADO DE ASTURIAS	53	416
COMUNIDAD AUTÓNOMA DE CANARIAS	92	602
LAS PALMAS	44	303
SANTA CRUZ DE TENERIFE	48	299
COMUNIDAD AUTÓNOMA DE CANTABRIA	49	453
COMUNIDAD AUTÓNOMA DE CASTILLA Y LEÓN	526	2.443
ÁVILA	9	40
BURGOS	98	361
LEÓN	166	814
PALENCIA	22	152
SALAMANCA	82	373
SEGOVIA	17	117
SORIA	10	37
VALLADOLID	85	385
ZAMORA	37	164
COMUNIDAD AUTÓNOMA DE CASTILLA-LA MANCHA	377	2.345
ALBACETE	75	395
CIUDAD REAL	108	563
CUENCA	84	664
GUADALAJARA	13	81
TOLEDO	97	642

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
COMUNIDAD AUTÓNOMA DE CATALUÑA	598	4.100
BARCELONA	334	2.563
GIRONA	63	585
LLEIDA	106	402
TARRAGONA	95	550
COMUNIDAD DE MADRID	141	1.671
COMUNIDAD VALENCIANA	415	3.723
ALICANTE	143	1.228
CASTELLÓN DE LA PLANA	92	649
VALENCIA	180	1.846
COMUNIDAD AUTÓNOMA DE EXTREMADURA	203	1.656
BADAJOZ	162	1.462
CÁCERES	41	194
COMUNIDAD AUTÓNOMA DE GALICIA	281	1.609
A CORUÑA	93	578
LUGO	58	293
OURENSE	64	430
PONTEVEDRA	66	308
COMUNIDAD AUTÓNOMA DE LAS ILLES BALEARS	71	758
COMUNIDAD FORAL DE NAVARRA	105	541
COMUNIDAD AUTÓNOMA DEL PAÍS VASCO	201	2.588
ÁLAVA	37	252
GUIPÚZCOA	87	1.497
VIZCAYA	77	839
COMUNIDAD AUTÓNOMA DE LA RIOJA	31	171
COMUNIDAD AUTÓNOMA DE LA REGIÓN DE MURCIA	41	589

* En esta tabla aparecen diferenciados por Provincias y Comunidades Autónomas, los ficheros de la Administración Local y Organismos Públicos de Entidades Locales.

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS

CÁMARAS OFICIALES DE COMERCIO E INDUSTRIA	335
NOTARIADO	5.905
UNIVERSIDADES	544
COLEGIOS PROFESIONALES	573
OTROS	229
TOTAL	7.586

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS

	2006	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS (IDEOLOGÍA, CREENCIAS, RELIGIÓN Y AFILIACIÓN SINDICAL)	283	3.878
OTROS DATOS ESPECIALMENTE PROTEGIDOS (ORIGEN RACIAL, SALUD Y VIDA SEXUAL)	885	8.022
DATOS RELATIVOS A INFRACCIONES	578	2.978
DATOS DE CARÁCTER IDENTIFICATIVO	5.486	56.138
DATOS DE CARACTERÍSTICAS PERSONALES	2.360	32.462
DATOS DE CIRCUNSTANCIAS SOCIALES	1.137	12.866
DATOS ACADÉMICOS Y PROFESIONALES	1.552	17.638
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	1.333	16.030
DATOS DE INFORMACIÓN COMERCIAL	864	9.263
DATOS ECONÓMICO-FINANCIEROS	2.302	26.963
DATOS DE TRANSACCIONES	741	7.886
OTROS TIPOS DE DATOS	16	53

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES

	2006	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	283	3.878
IDEOLOGÍA	71	194
CREENCIAS	13	72
RELIGIÓN	19	206
AFILIACIÓN SINDICAL	209	3.536
OTROS DATOS ESPECIALMENTE PROTEGIDOS	885	8.022
ORIGEN RACIAL	101	573
SALUD	874	7.982
VIDA SEXUAL	44	698
DATOS RELATIVOS A INFRACCIONES	578	2.978
INFRACCIONES PENALES	160	1.253
INFRACCIONES ADMINISTRATIVAS	563	2.610

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD

	2006	TOTAL
RECURSOS HUMANOS	719	11.399
GESTIÓN DE NÓMINA	382	4.138
PREVENCIÓN DE RIESGOS LABORALES	202	657
HACIENDA PÚBLICA Y GESTIÓN DE ADMINISTRACIONES TRIBUTARIAS	681	8.205
GESTIÓN ECONÓMICO-FINANCIERA PÚBLICA	382	5.209
GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA	1.047	12.430
JUSTICIA	167	1.653
SEGURIDAD PÚBLICA Y DEFENSA	191	2.884
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES POLICIALES	108	2.370
VIDEOVIGILANCIA	--	--
TRABAJO Y GESTIÓN DE EMPLEO	348	4.075
SERVICIOS SOCIALES	552	5.609
GESTIÓN Y CONTROL SANITARIO	239	3.049
HISTORIAL CLÍNICO	85	1.544
INVESTIGACIÓN EPIDEMIOLÓGICA Y ACTIVIDADES ANÁLOGAS	60	1.736
EDUCACIÓN Y CULTURA	629	5.740
FUNCIÓN ESTADÍSTICA PÚBLICA	389	9.221
PADRÓN DE HABITANTES	261	5.017
GESTIÓN DEL CENSO PROMOCIONAL	--	--
FINES CIENTÍFICOS, HISTÓRICOS O ESTADÍSTICOS	1.123	15.598
SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS	77	1.953
PROCEDIMIENTO ADMINISTRATIVO	2.158	19.522
PUBLICACIONES	122	1.043
GESTIÓN SANCIONADORA	359	3.408
PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA	246	939
OTRAS FINALIDADES	1.129	9.273

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN LA PROCEDENCIA DE LOS DATOS

PROCEDENCIA DE LOS DATOS	2006	TOTAL
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	5.215	53.363
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	1.176	11.232
FUENTES ACCESIBLES AL PÚBLICO	227	3.915
REGISTROS PÚBLICOS	843	8.979
ENTIDAD PRIVADA	451	8.108
ADMINISTRACIONES PÚBLICAS	1.888	19.553

FICHEROS CON CESIONES DE DATOS

INSCRITOS EN 2006	TOTAL
2.245	31.180

TRANSFERENCIAS INTERNACIONALES DE DATOS

**RESOLUCIONES DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES
A TERCEROS PAÍSES CON NIVEL DE PROTECCIÓN NO ADECUADO (ART. 33 LOPD)**

PAÍSES DESTINATARIOS DE LA AUTORIZACIÓN DE TRANSFERENCIA INTERNACIONAL

	2000	2001	2002	2003	2004	2005	2006	TOTAL
EEUU	1	9	2	6	40	9	16	83
MARRUECOS	1	-	-	-	2	2	2	7
ARGENTINA ⁴	-	-	2	-	-	-	-	2
INDIA	-	-	-	-	4	-	3	7
SINGAPUR	-	-	-	-	1	-	1	2
JAPÓN	-	-	-	-	-	1	-	1
PANAMÁ	-	-	-	-	-	2	-	2
COLOMBIA	-	-	-	-	-	1	4	5
MALASIA	-	-	-	-	-	1	1	2
TAILANDIA	-	-	-	-	-	1	-	1
CHILE	-	-	-	-	-	1	7	8
URUGUAY	-	-	-	-	-	1	1	2
FILIPINAS	-	-	-	-	-	-	3	3
PERÚ	-	-	-	-	-	-	4	4
CHINA	-	-	-	-	-	-	1	1
HONG KONG	-	-	-	-	-	-	1	1
GUATEMALA	-	-	-	-	-	-	1	1
PARAGUAY	-	-	-	-	-	-	1	1
TOTALES	2	9	4	6	47	19	46	133
TOTAL RESOLUCIONES DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES DEL DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS INSCRITAS EN EL RGPD ⁵								131

⁴ Las Autorizaciones de Transferencia Internacional con destino a Argentina se tramitaron con anterioridad a la Decisión de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

⁵ Resoluciones tramitadas de conformidad con la LOPD. El número de resoluciones de autorización no coincide con el número de países destinatarios de la autorización debido a que una misma resolución puede autorizar transferencias a distintos países.

TRANSFERENCIAS INTERNACIONALES DE DATOS

FICHEROS INSCRITOS QUE DECLARAN TRANSFERENCIAS INTERNACIONALES

	TOTAL FICHEROS CON TRANSFERENCIAS
TITULARIDAD PÚBLICA	186
TITULARIDAD PRIVADA	8.185
TOTAL	8.311

DERECHO DE CONSULTA AL REGISTRO

DATOS SOBRE CONSULTAS AL APARTADO FICHEROS INSCRITOS EN LA WEB

TITULARIDAD	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
PRIVADA	17.410	63.896	90.923	69.274	82.443	76.255	60.009	36.535	76.466	46.410	69.571	51.897	741.089
PÚBLICA	2.806	17.847	57.946	42.274	76.797	18.413	15.411	12.804	17.709	17.709	15.727	20.118	315.561
TOTAL	20.216	81.743	148.869	111.548	159.340	94.668	75.420	49.339	94.065	64.119	75.298	72.015	1.056.650

ACCESOS AL CANAL DEL RESPONSABLE EN LA WEB

DOCUMENTO	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
FORMULARIO NOTA PRIVADO	--	--	--	--	--	--	--	--	2.852	1.344	6.779	6.155	17.130
FORMULARIO NOTA PÚBLICO	--	--	--	--	--	--	--	--	805	238	1.078	878	2.999
PROGRAMA DE AYUDA PRIVADO	540	1.990	3.020	2.003	2.480	2.259	1.760	1.275	2.251	1.239	1.082	251	20.150
PROGRAMA DE AYUDA PÚBLICO	79	301	389	292	426	353	303	184	331	173	197	63	3.091
FORMULARIO PRIVADO	239	1.370	2.003	1.357	1.695	1.577	1.354	902	1.766	933	262	--	13.458
FORMULARIO PÚBLICO	60	296	439	331	351	346	271	179	359	158	33	--	2.823
DOCUMENTO DE SEGURIDAD	836	3.006	4.797	3.034	3.668	3.284	2.753	1.830	2.799	1.644	3.136	2.167	32.954

ESTADÍSTICAS RELATIVAS AL REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTACIÓN

REGISTRO DE DOCUMENTACIÓN

	2000	2001		2002		2003		2004		2005		2006	
REGISTRO DE ENTRADA	3.260	4.232	30%	5.855	38%	5.394	-8%	7.013	30%	9.155	31%	10.087	10%
REGISTRO DE SALIDA	3.080	4.406	43%	5.152	17%	5.120	-1%	6.786	33%	8.824	30%	10.073	14%
TOTALES	6.340	8.638	36%	11.007	27%	10.514	-4%	13.799	31%	17.979	30%	20.160	12%

ESTADÍSTICAS RELATIVAS A ACTUACIONES Y PROCEDIMIENTOS INICIADOS Y FINALIZADOS

ACTUACIONES Y PROCEDIMIENTOS INICIADOS (ÁREA DE INSPECCIÓN)

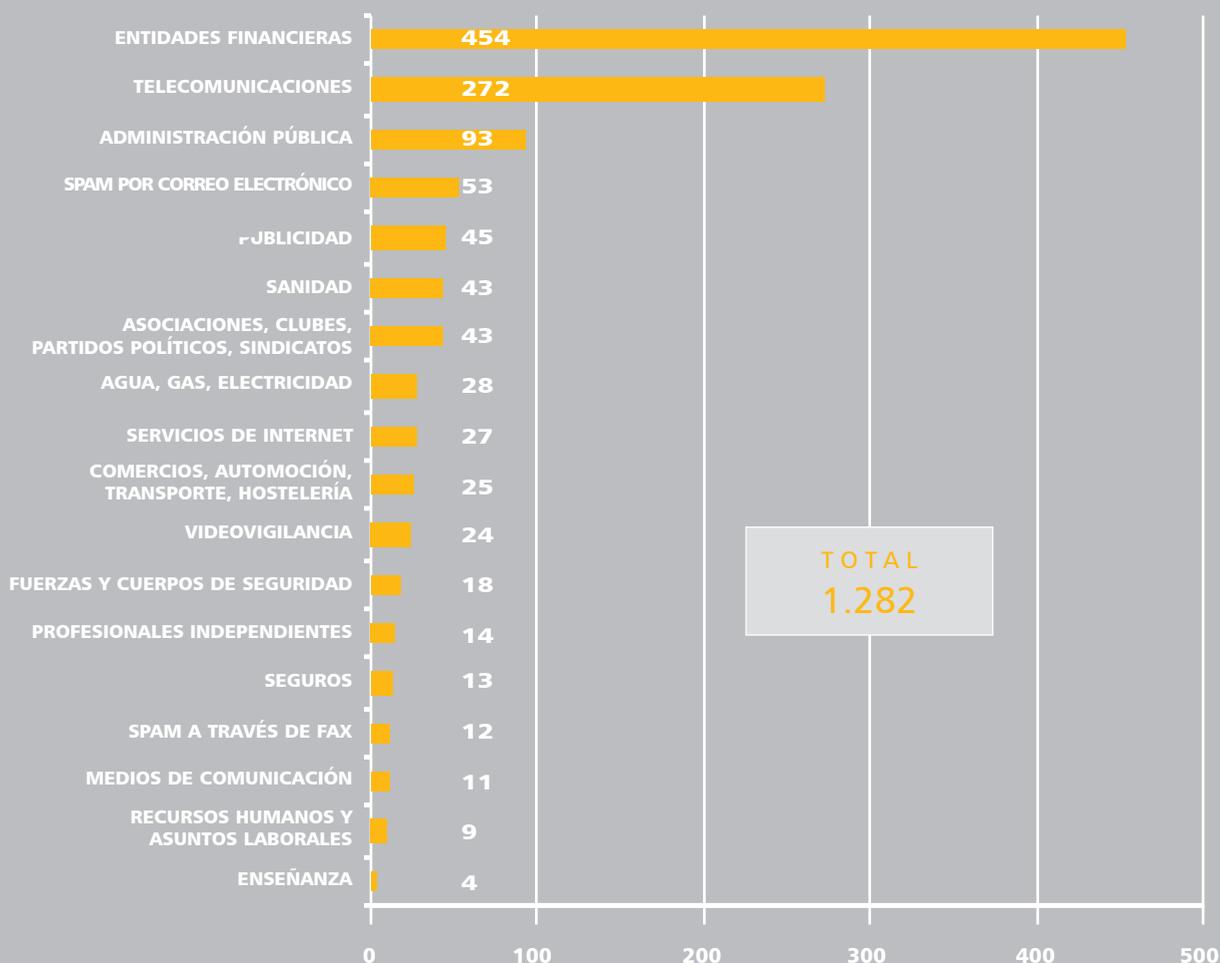
ACTUACIONES PREVIAS DE INVESTIGACIÓN	2000	2001		2002		2003		2004		2005		2006	
	319	405	27%	723	79%	574	21%	978	70%	1.158	18%	1.282	11%

ACTUACIONES Y PROCEDIMIENTOS FINALIZADOS (ÁREA DE INSTRUCCIÓN)

	2003	2004	2005	2006
ARCHIVO DIRECTO TRAS INVESTIGACIÓN	218	374	368	370
PROCEDIMIENTO SANCIONADOR (CULMINA EN SANCIÓN O EXONERACIÓN)	148	189	279	301
ADMINISTRACIONES PÚBLICAS (CULMINA EN DECLARACIÓN O EXONERACIÓN)	16	31	20	107
RECURSOS DE REPOSICIÓN	114	127	197	205
TUTELAS DE DERECHO	541	463	592	556
TOTALES	1.037	1.184	1.456	1.539

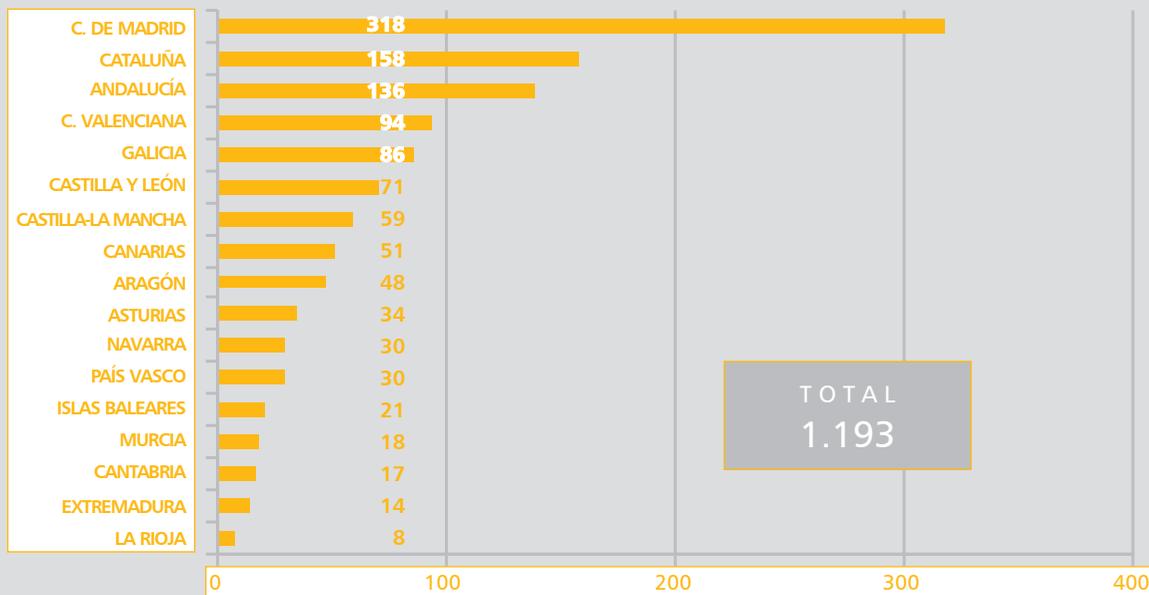
ACTUACIONES PREVIAS DE INVESTIGACIÓN

Tras la decisión del Director de abrir un expediente, bien a consecuencia de la recepción de una denuncia o bien de oficio al tener conocimiento de alguna actuación presuntamente contraria a la normativa vigente en materia de protección de datos, se realiza una investigación con objeto de determinar los hechos susceptibles de motivar la iniciación de un procedimiento sancionador, así como la identificación de los presuntos responsables. Esta investigación puede conllevar la realización de inspecciones "in situ" a efectos de examinar los equipos y ficheros utilizados en el tratamiento de datos. Es realizada por la Unidad de Inspección, que forma parte de la Subdirección.

**ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006
POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO**


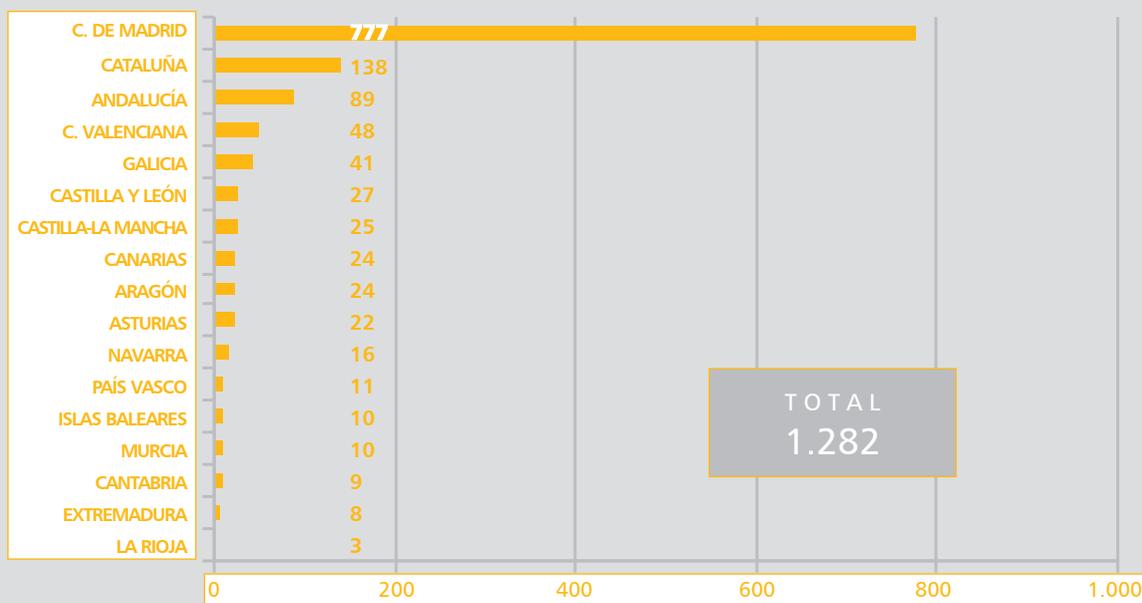
ACTUACIONES PREVIAS DE INVESTIGACIÓN

ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL DENUNCIANTE

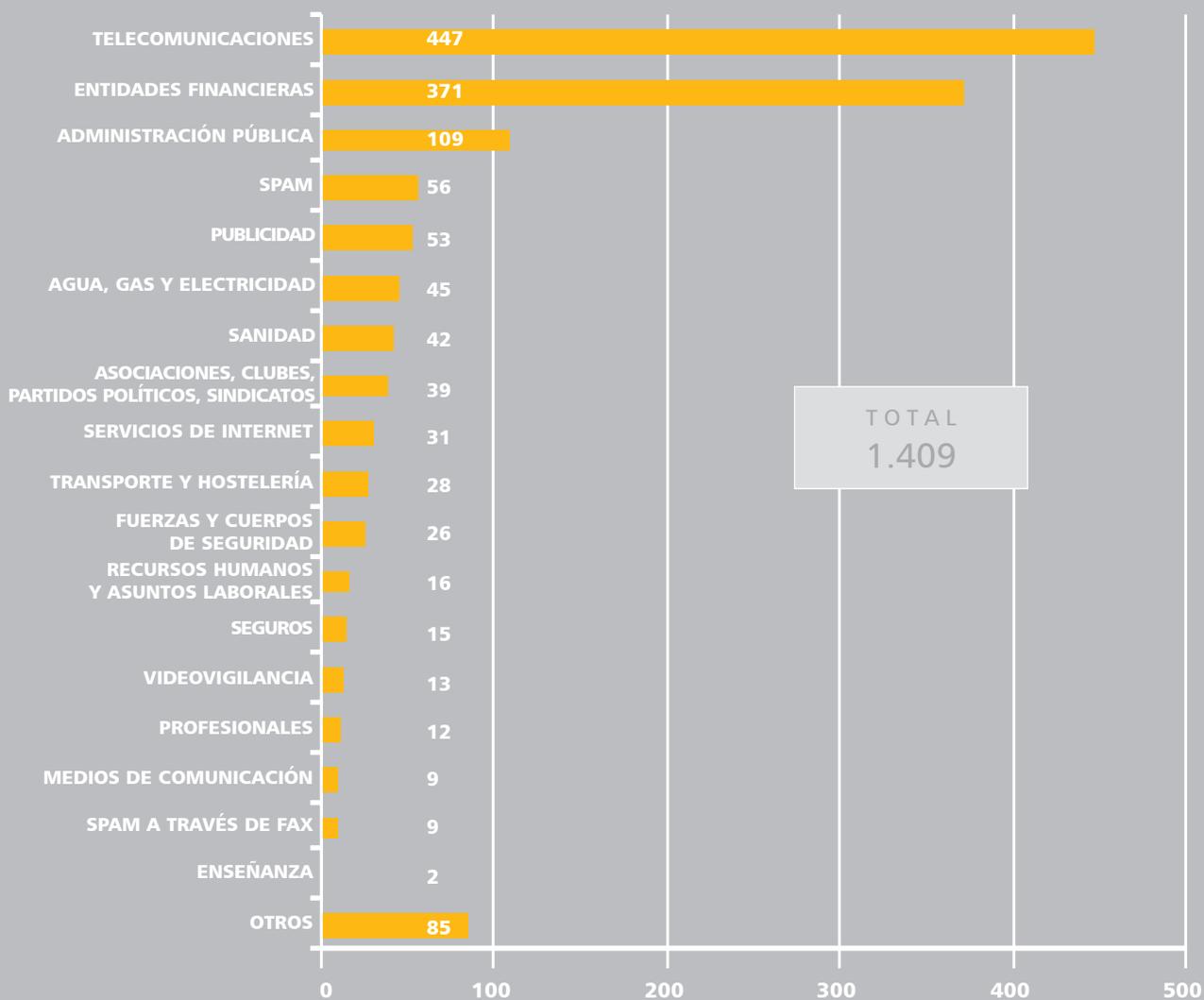


No se incluyen las actuaciones iniciadas de oficio, sin denuncia previa, provenientes del extranjero y otros. En 2006 se iniciaron 8 actuaciones como consecuencia de denuncias procedentes del exterior.

ACTUACIONES PREVIAS DE INVESTIGACIÓN INICIADAS EN 2006 POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL INVESTIGADO



ACTUACIONES PREVIAS DE INVESTIGACIÓN

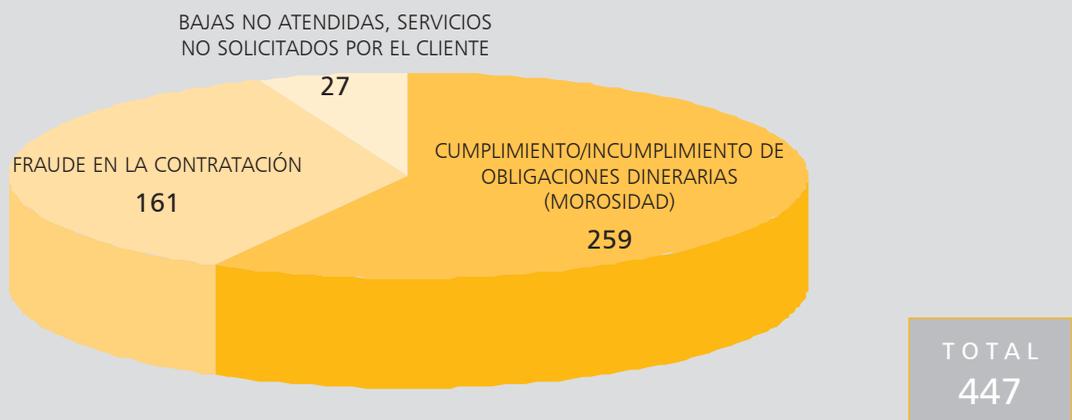
ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006
POR SECTOR DE ACTIVIDAD DEL PRINCIPAL INVESTIGADO

ACTUACIONES PREVIAS DE INVESTIGACIÓN

ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR FINANCIERO



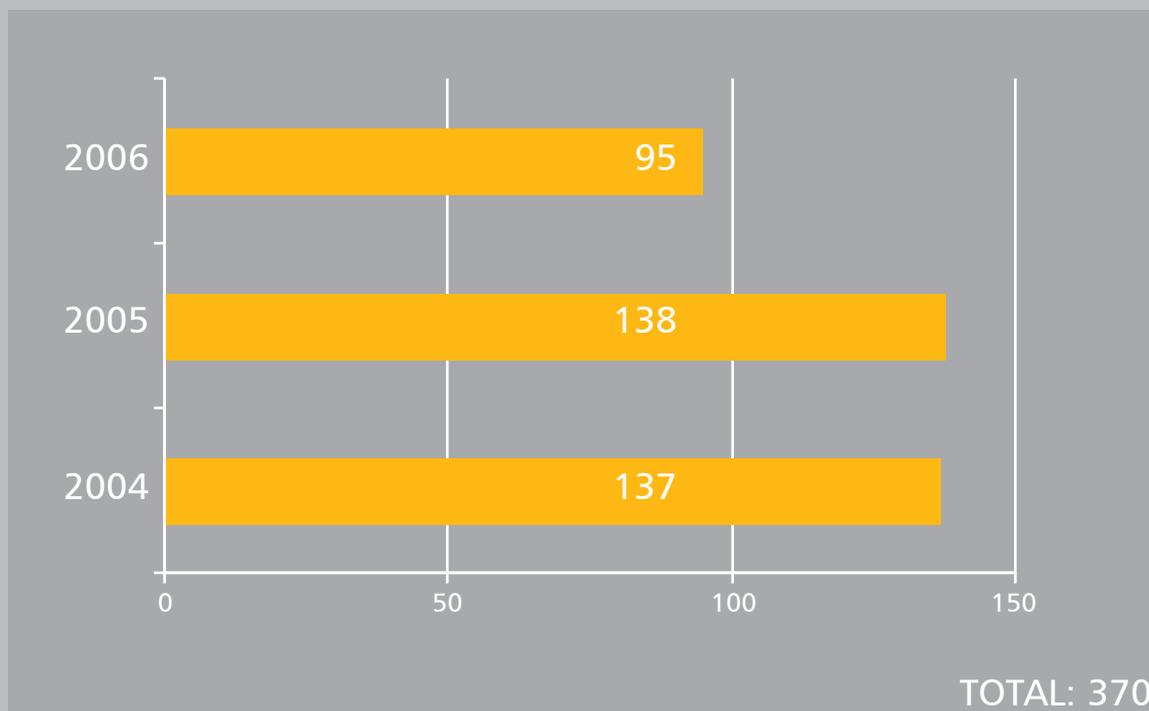
ACTUACIONES PREVIAS DE INVESTIGACIÓN FINALIZADAS EN 2006 DEL SECTOR TELECOMUNICACIONES



ACTUACIONES POSTERIORES A LA INSPECCIÓN

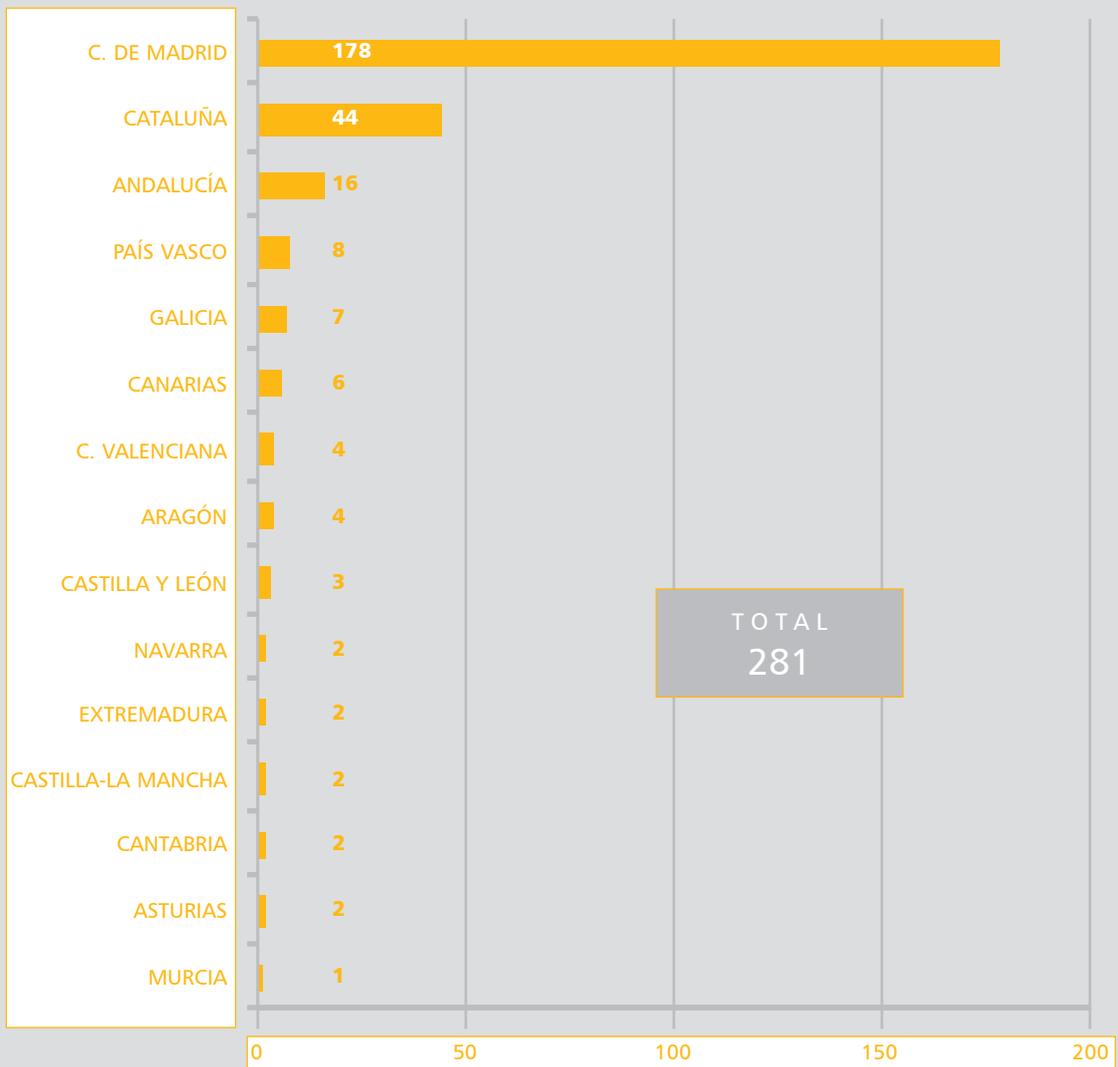
Finalizada la investigación, el expediente se remite a la Unidad de Instrucción, también dependiente de la Subdirección, a los efectos de presentar al Director la propuesta de archivar las actuaciones por no existir indicios de infracción o, por el contrario, la apertura de un procedimiento sancionador o de declaración de infracción de las Administraciones Públicas, dependiendo si el presunto responsable es de naturaleza privada o pública. Una vez acordado por el Director el inicio del procedimiento, la Unidad de Instrucción es el órgano competente para realizar su tramitación.

RESOLUCIONES DE ARCHIVO

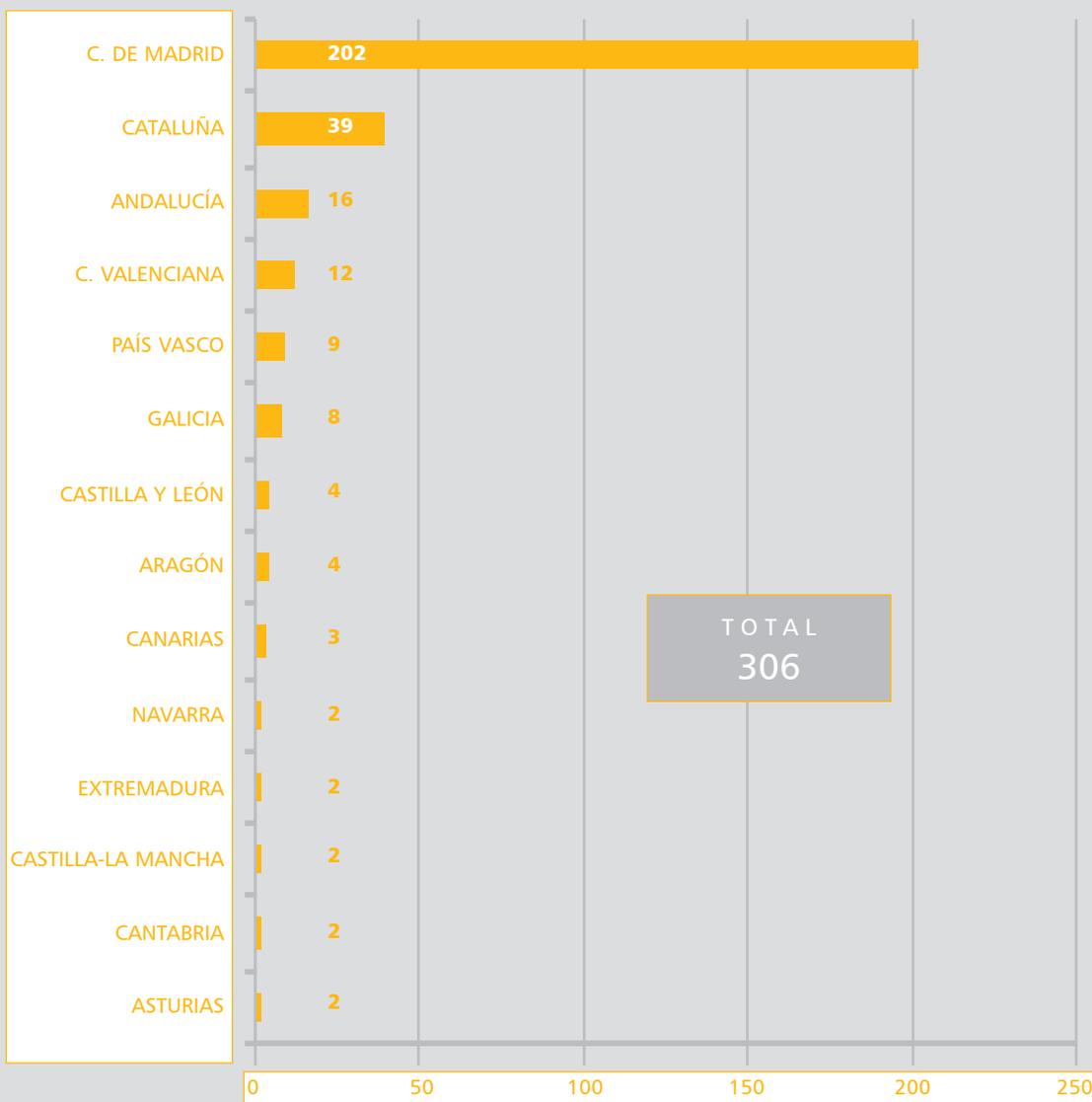


Se desglosan las resoluciones de archivo en función del ejercicio en el que se iniciaron las actuaciones de inspección (investigación previa).

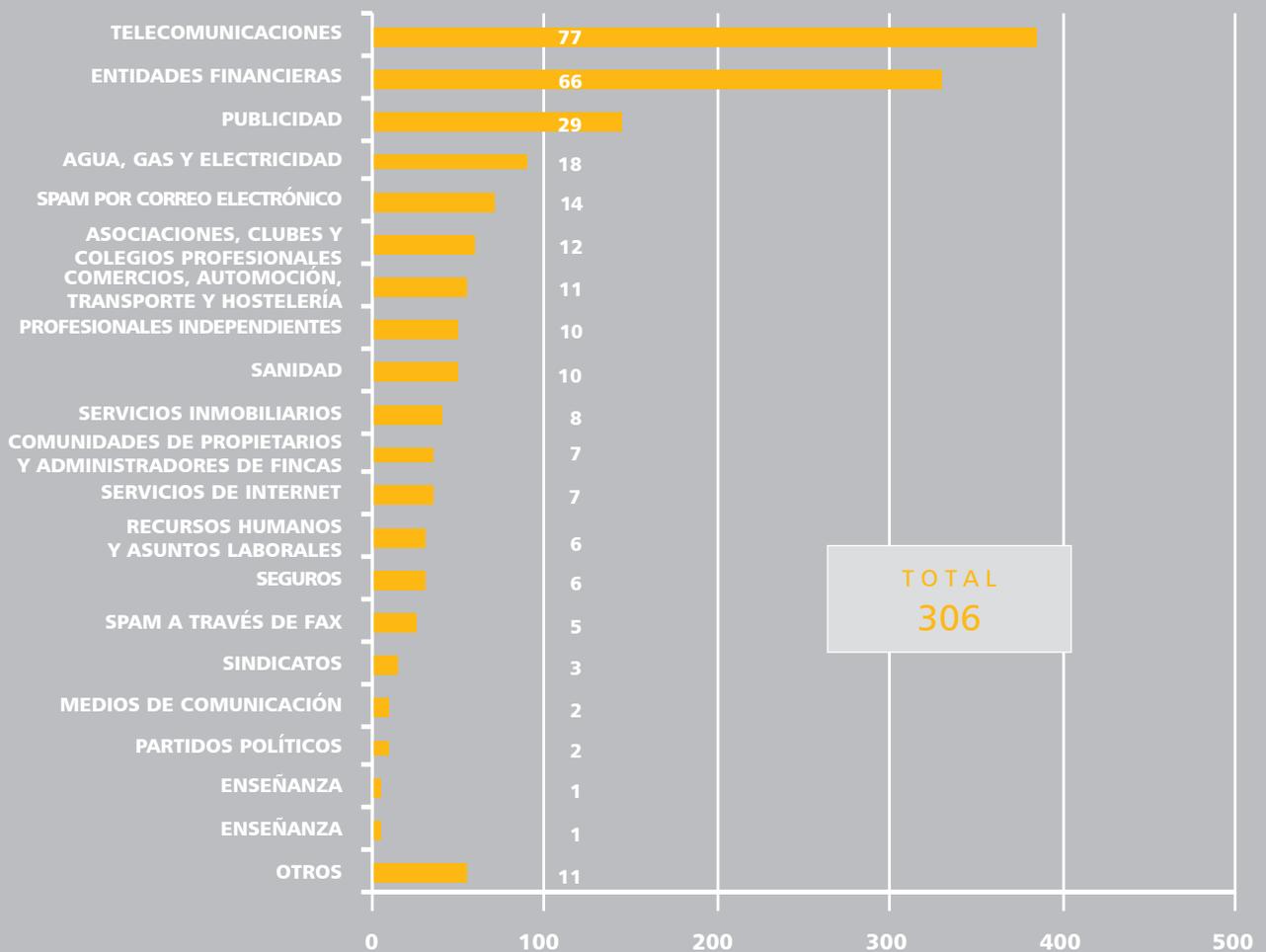
ACTUACIONES POSTERIORES A LA INSPECCIÓN

PROCEDIMIENTOS SANCIONADORES INICIADOS EN 2006
POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO

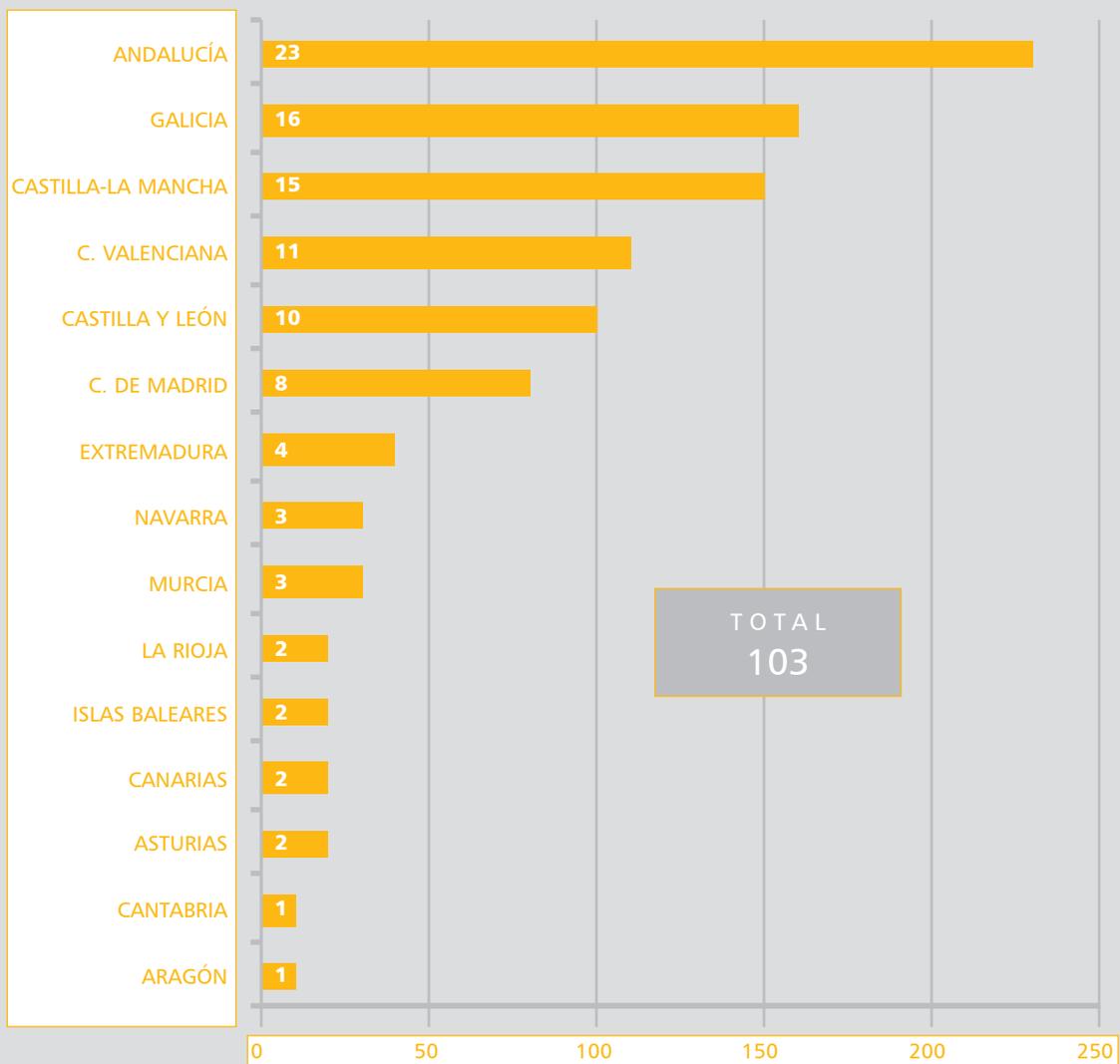
ACTUACIONES POSTERIORES A LA INSPECCIÓN

PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006
POR COMUNIDAD AUTÓNOMA DEL PRINCIPAL IMPUTADO

ACTUACIONES POSTERIORES A LA INSPECCIÓN

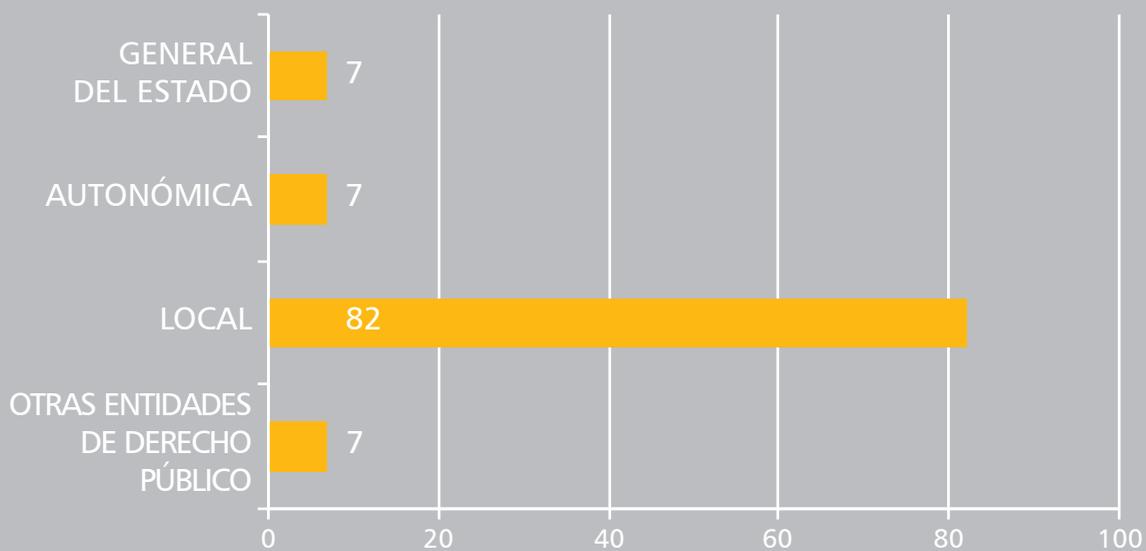
PROCEDIMIENTOS SANCIONADORES FINALIZADOS EN 2006
POR SECTOR DE ACTIVIDAD DEL PRINCIPAL IMPUTADO

ACTUACIONES POSTERIORES A LA INSPECCIÓN

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR COMUNIDAD AUTÓNOMA EN LA QUE RADICA LA ADMINISTRACIÓN IMPUTADA

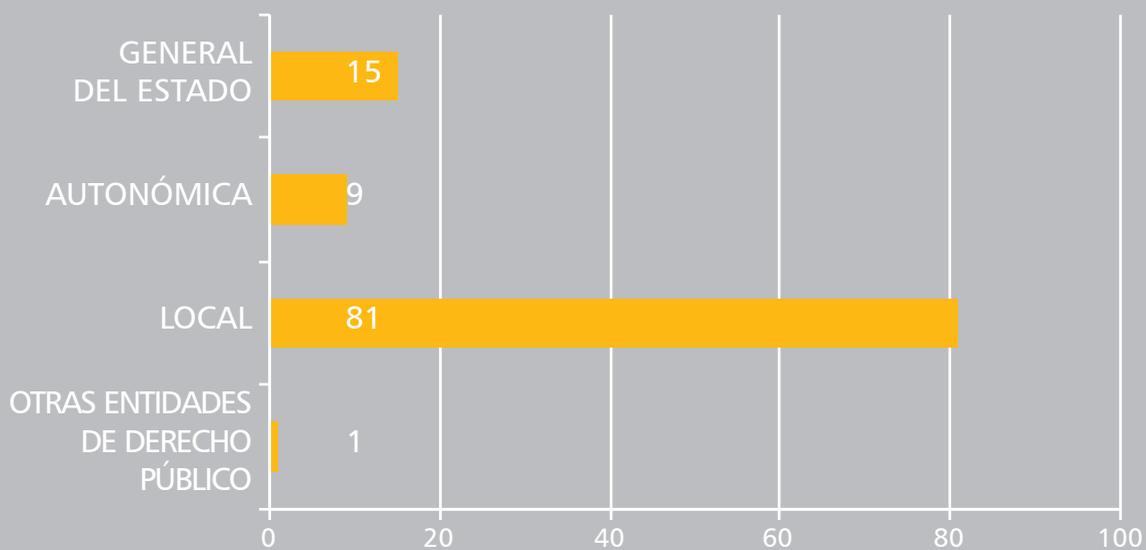
ACTUACIONES POSTERIORES A LA INSPECCIÓN

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS INICIADOS POR TIPO DE ADMINISTRACIÓN



TOTAL: 103

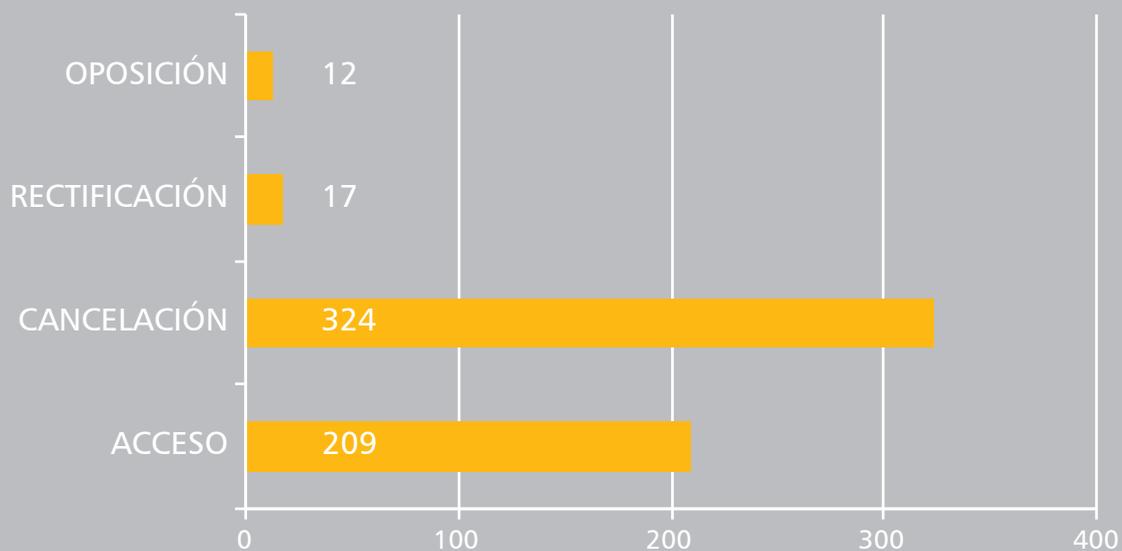
PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS FINALIZADOS POR TIPO DE ADMINISTRACIÓN



TOTAL: 106

TUTELAS DE DERECHOS

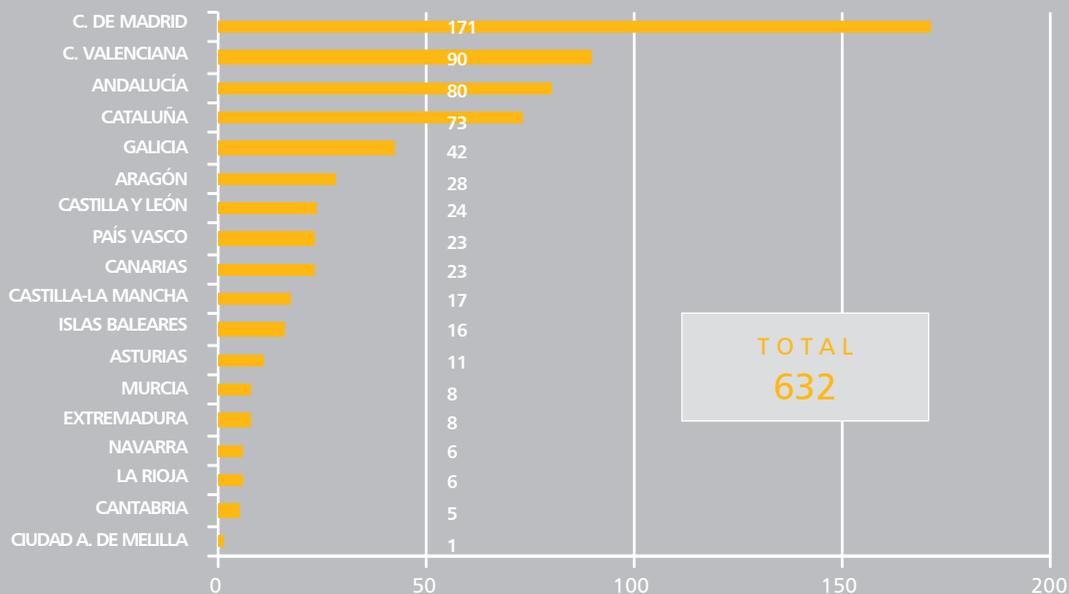
PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR DERECHO TUTELADO



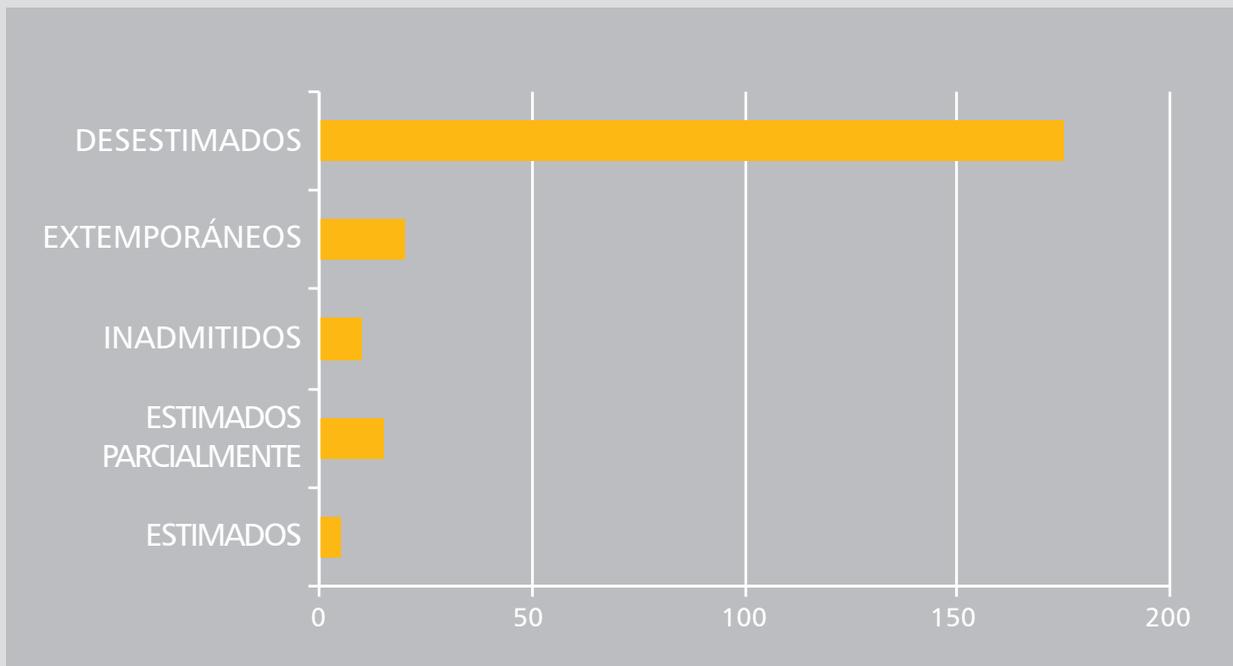
TOTAL DERECHOS TUTELADOS: 563

TOTAL PROCEDIMIENTOS: 556

PROCEDIMIENTOS DE TUTELA DE DERECHOS POR COMUNIDAD AUTÓNOMA DEL RECLAMANTE

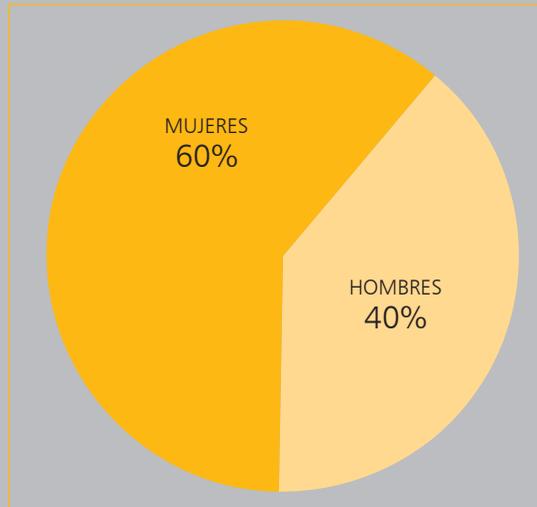


RECURSOS DE REPOSICIÓN

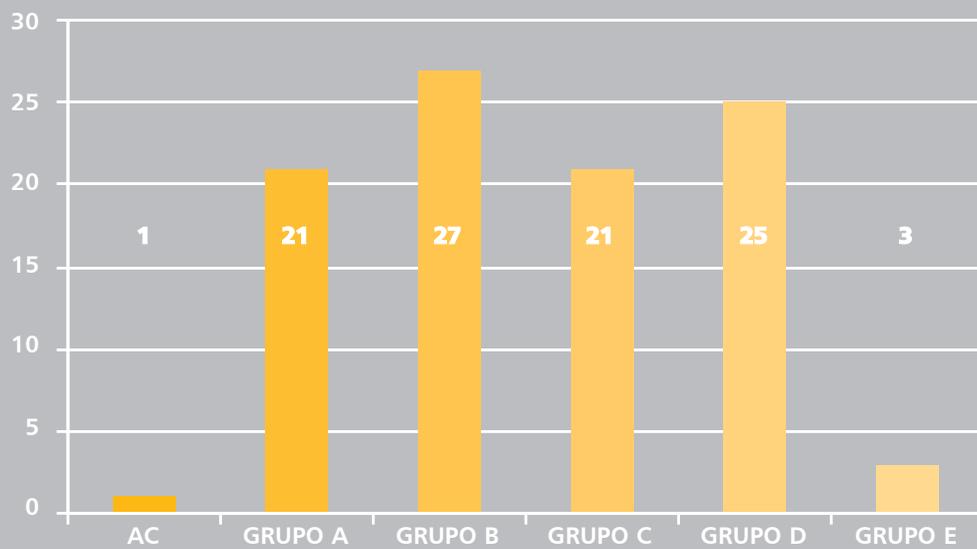


RECURSOS HUMANOS

EFFECTIVOS DE LA AGPD POR SEXO

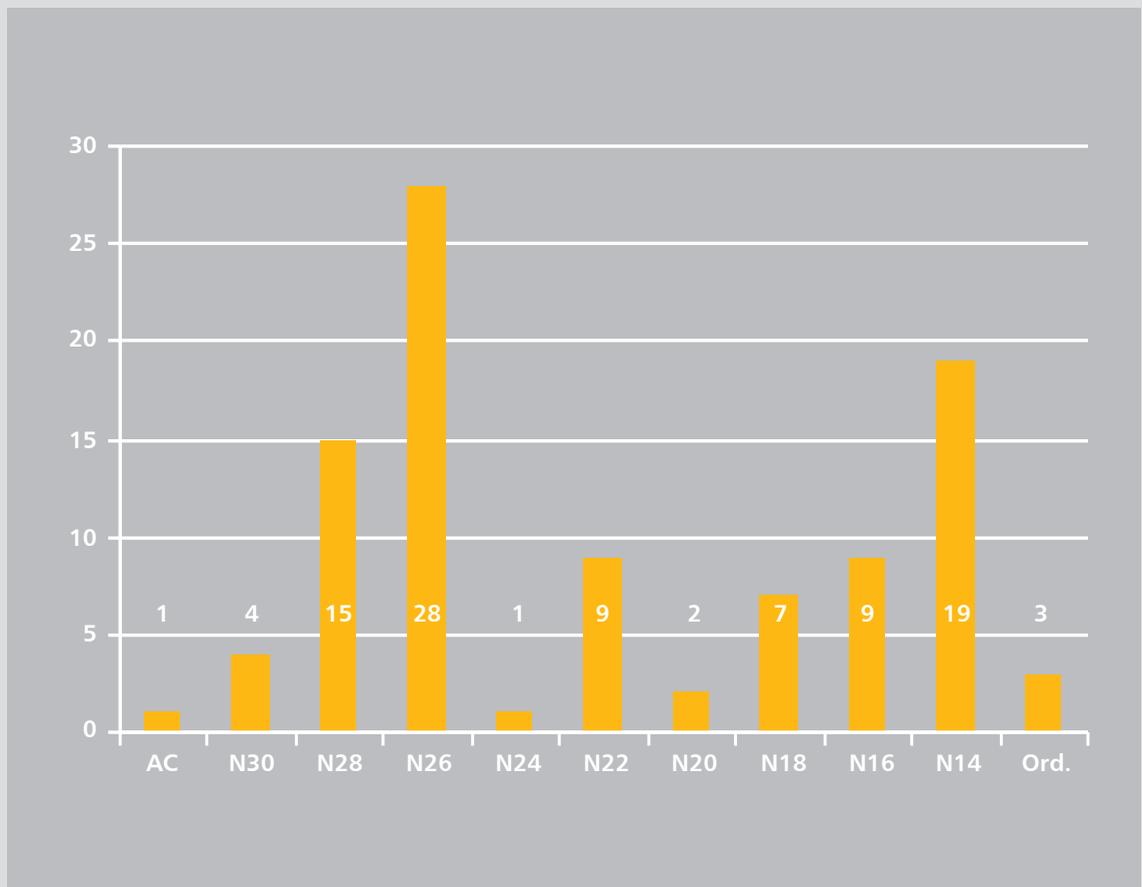


RELACIÓN DE EFFECTIVOS POR GRUPOS



RECURSOS HUMANOS

RELACIÓN DE EFECTIVOS POR NIVELES



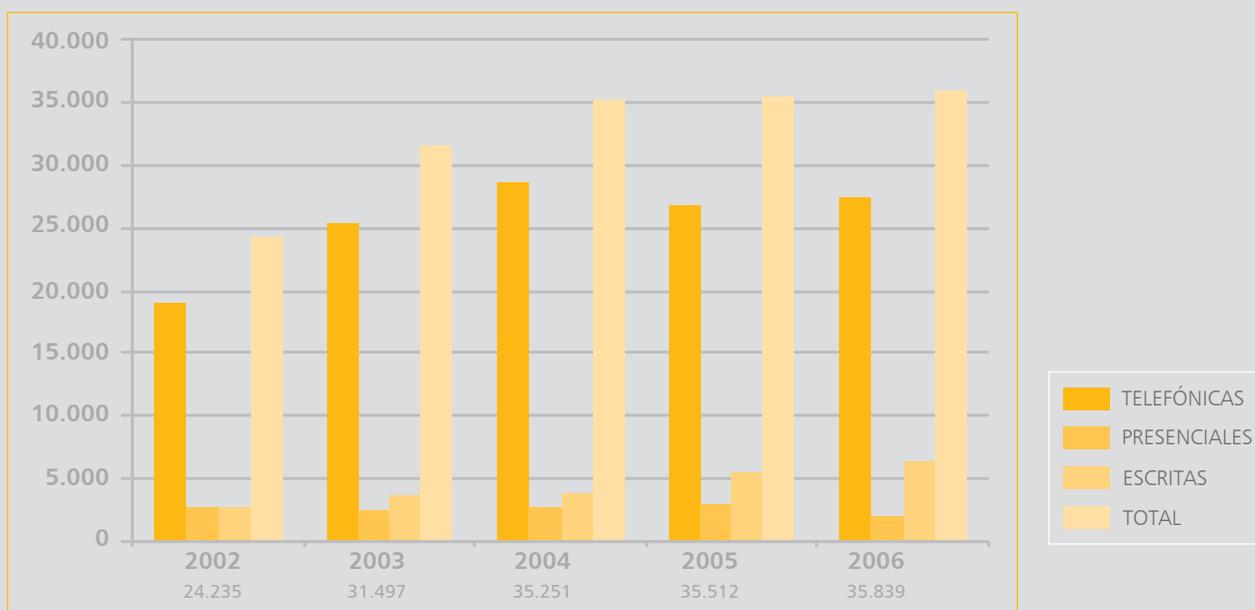
ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

AÑO	ATENCIÓN TELEFÓNICA	ATENCIÓN PRESENCIAL	ATENCIÓN POR ESCRITO	TOTAL	PORCENTAJE DE INCREMENTO
2002	18.870	2.722	2.643	24.235	21,53%
2003	25.326	2.421	3.750	31.497	29,90%
2004	28.661	2.766	3.824	35.251	11,92%
2005	26.654	2.938	5.420	35.512	1,53%
2006	27.486	2.030	6.323 *	35.839	0,9%

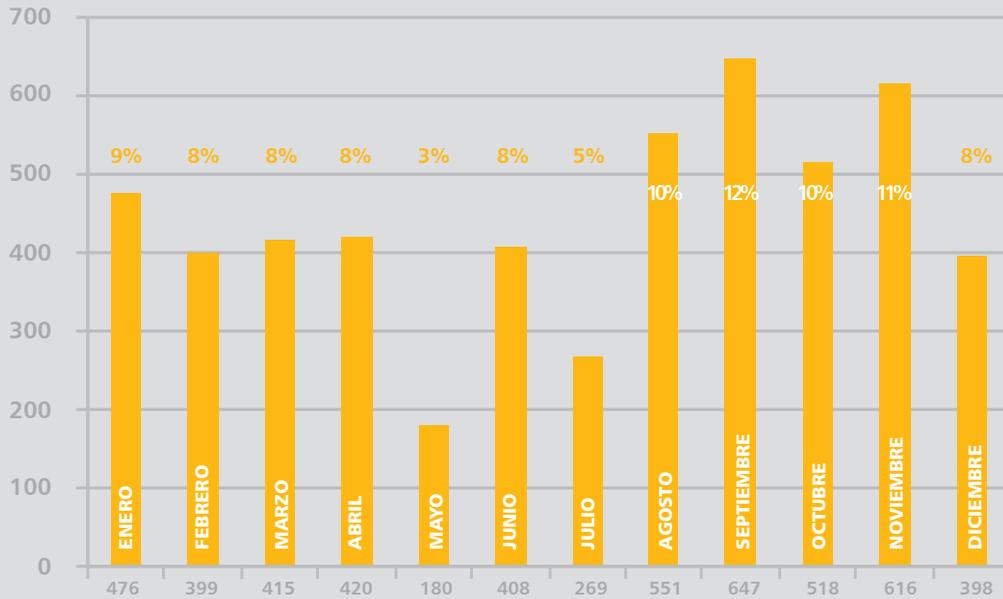
* En el año 2006, 5.534 consultas escritas se contestaron a través de la página Web.

COMPARACIÓN CON AÑOS ANTERIORES



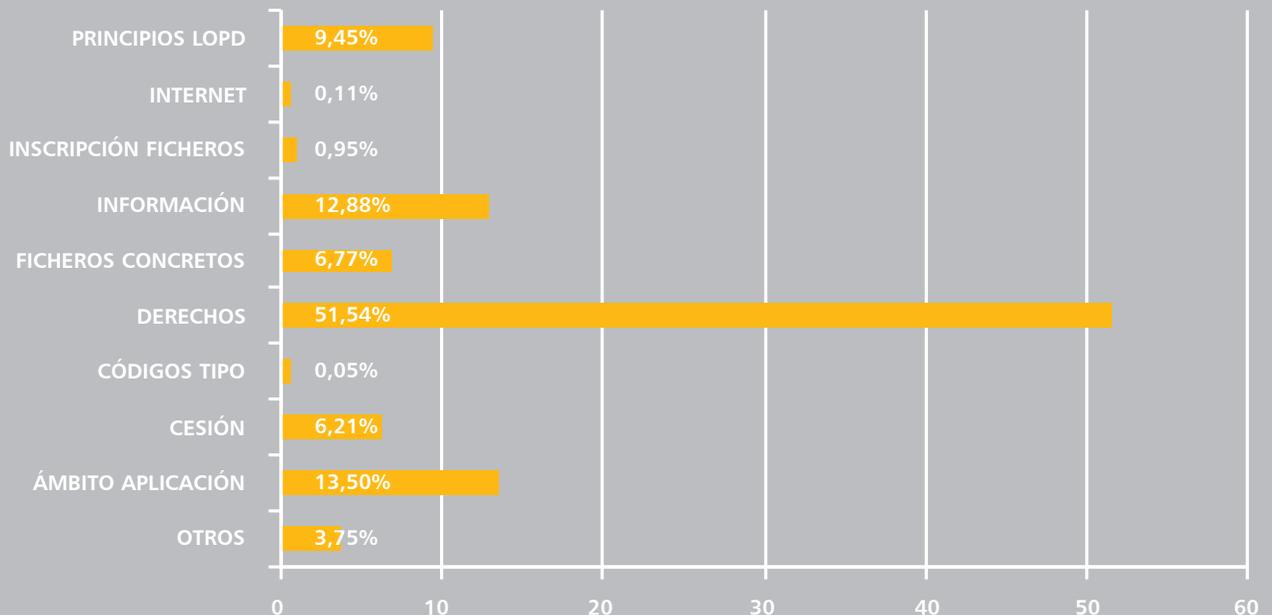
ATENCIÓN AL CIUDADANO

EVOLUCIÓN DE LAS CONSULTAS PLANTEADAS A TRAVÉS DE INTERNET



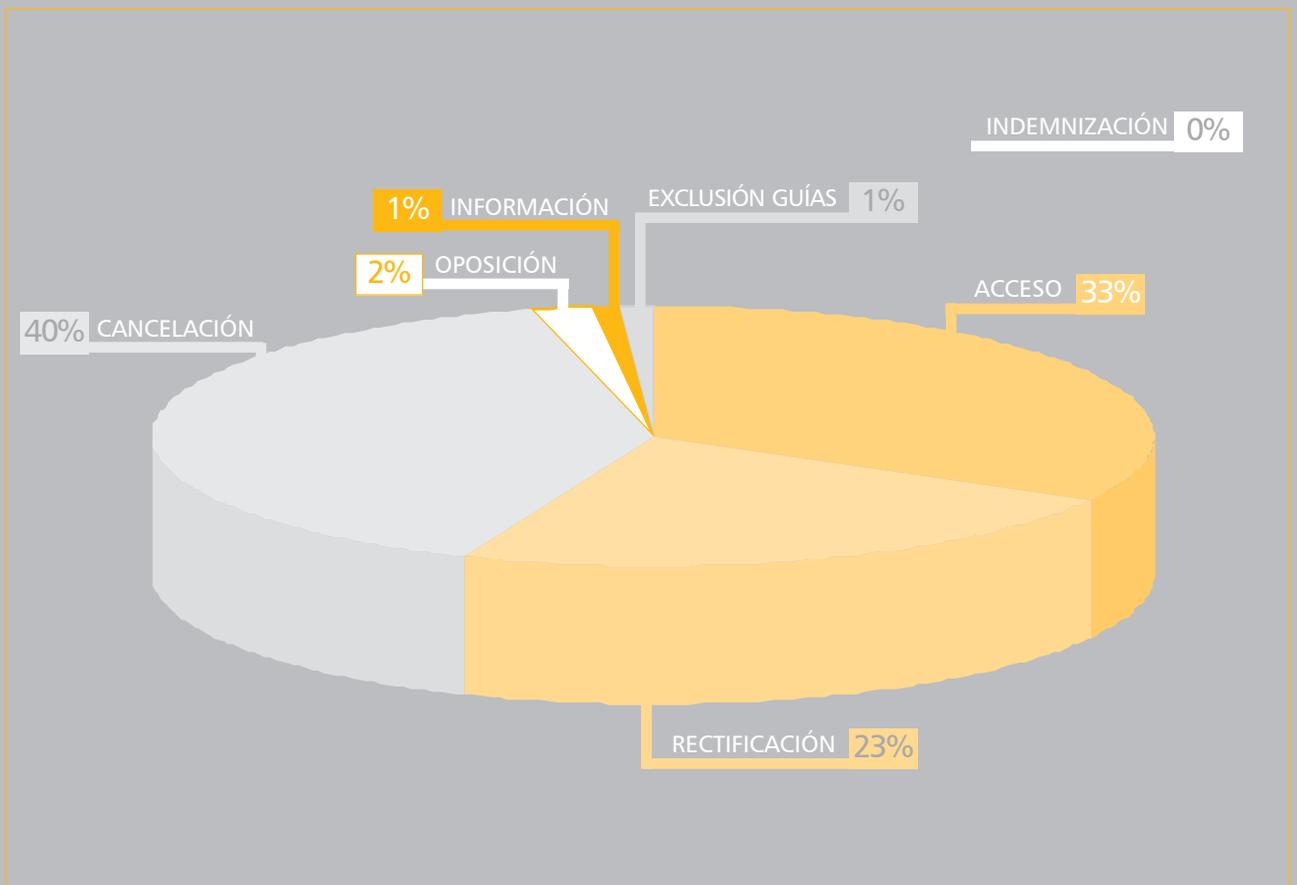
* Durante el año 2006 el número total de consultas realizadas por este medio fue de 5.534, repartidas gráficamente del siguiente modo.

ANÁLISIS DE LAS CONSULTAS POR TEMAS 2006



ATENCIÓN AL CIUDADANO

EXAMEN DEL APARTADO SOBRE DERECHOS 2006

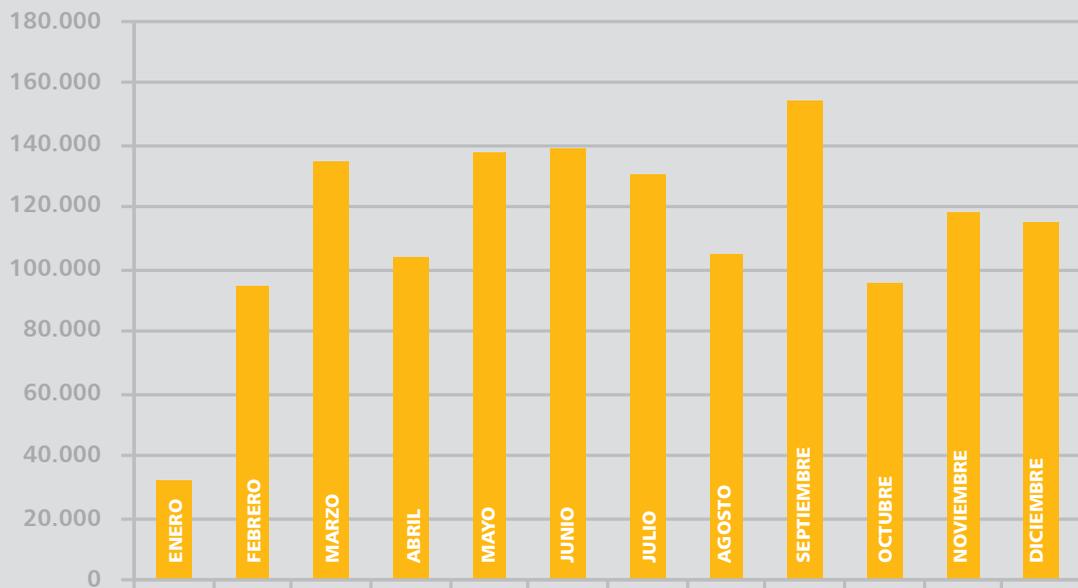


ATENCIÓN AL CIUDADANO

ACCESOS A LA PÁGINA WEB AÑO 2006

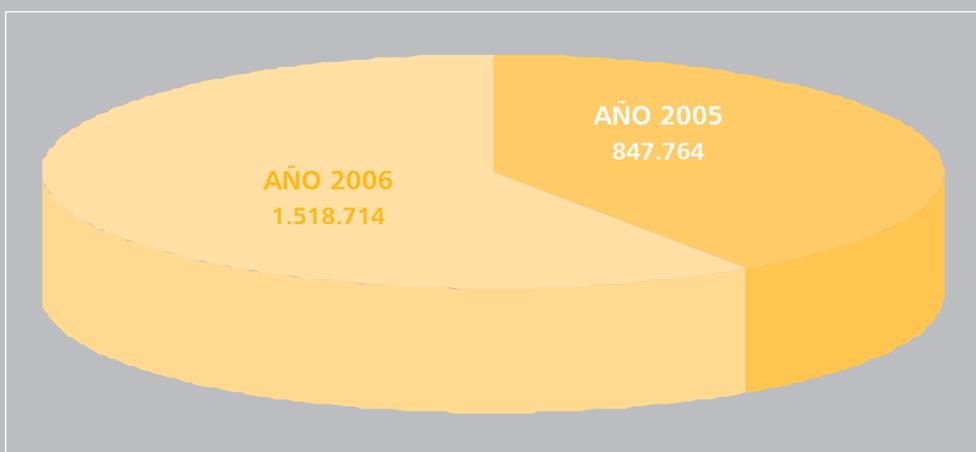
ENERO	31.492
FEBRERO	94.652
MARZO	135.254
ABRIL	103.413
MAYO	137.893
JUNIO	138.421
JULIO	130.665
AGOSTO	105.337
SEPTIEMBRE	153.835
OCTUBRE	96.105
NOVIEMBRE	118.231
DICIEMBRE	114.808
TOTAL	1.538.714

EVOLUCIÓN GRÁFICA DE LOS ACCESOS WEB DURANTE EL AÑO 2006

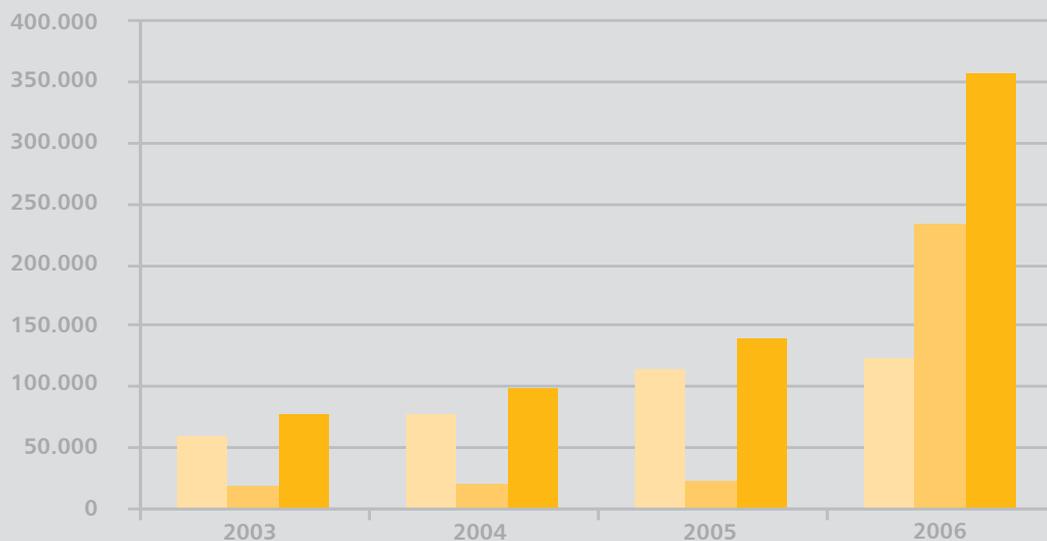


ATENCIÓN AL CIUDADANO

COMPARATIVA ACCESOS WEB 2005-2006



ATENCIÓN AL CIUDADANO

REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006
COMPARATIVA CON AÑOS ANTERIORES

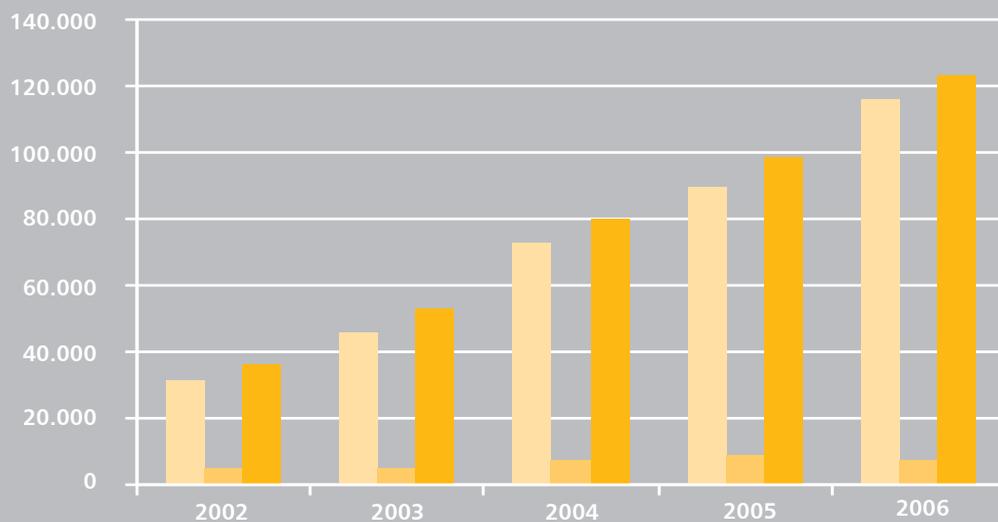
AÑOS	ENTRADAS	SALIDAS	TOTALES	% DE INCREMENTO
2003	59.642	18.118	77.760	21,42
2004	76.603	20.265	98.868	27,14
2005	114.563	23.977	138.540	40,12
2006	124.362*	233.109**	357.471	155

* El número de entradas en toda la Agencia. El Área de Atención al Ciudadano realizó 116.318.

** Este número representa las salidas registradas en toda la Agencia. El Área de Atención al Ciudadano registró 7.144. Ello obedece a que se permitió, durante el año 2006, registrar salidas a las distintas Unidades de la Agencia, dado que en Atención al Ciudadano no eran asumibles por su elevado volumen.

ATENCIÓN AL CIUDADANO

REGISTROS DE ENTRADA Y SALIDA DE DOCUMENTOS 2006 EN EL ÁREA DE ADMINISTRACIÓN GENERAL Y ATENCIÓN AL CIUDADANO. COMPARATIVA CON AÑOS ANTERIORES



AÑOS	ENTRADAS	SALIDAS	TOTALES	% DE INCREMENTO
2002	30.811	4.985	35.796	1.115,48
2003	45.577	5.036	52.613	46,98
2004	72.590	7.421	80.011	52,07
2005	89.520	8.759	98.279	22,83
2006	116.318	7.144	123.462	25,62

GESTIÓN ECONÓMICA

**PRESUPUESTO DE INGRESOS
(PREVISIÓN DEFINITIVA EN EUROS)**

CAPÍTULOS	2002	2003	2004	2005	2006
Multas y Sanciones	1.299.130,00	1.502.520,00	1.858.120,00	2.000.000,00	2.200.000,00
Transferencias corrientes	1.917.770,00	0,00	240.000,00	242.000,00	242.000,00
Ingresos patrimoniales	240.400,00	240.400,00	250.000,00	250.000,00	275.000,00
Enajenación inversiones reales	0,00	0,00	0,00	0,00	0,00
Transferencias capital	192.320,00	0,00	0,00	0,00	0,00
Remanente de Tesorería	922.247,38	3.195.975,67	3.256.720,10	4.898.736,37	7.059.418,58
TOTALES	4.571.867,38	4.938.895,67	5.604.840,10	7.390.736,37	9.776.418,58

ANÁLISIS CAPÍTULO "MULTAS Y SANCIONES" SOBRE DERECHOS RECONOCIDOS (EN EUROS)

AÑOS	DERECHOS RECONOCIDOS	RECAUDACIÓN TOTAL	PORCENTAJE RECAUDADO
2002	7.989.166,22	4.258.190,45	53,30
2003	8.372.379,74	5.486.738,23	65,53
2004	16.439.801,58	7.193.555,09	45,13
2005	21.105.083,99	9.577.950,09	45,38
2006	24.422.292,48	12.232.381,23	50,09

GESTIÓN ECONÓMICA

PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULO

AÑOS	PRESUPUESTO INICIAL	MODIFICACIONES	%	PRESUPUESTO DEFINITIVO
2002	4.310.510,00	261.357,38	6,06	4.571.867,38
2003	4.777.180,00	161.715,67	3,39	4.938.895,67
2004	5.386.510,00	216.330,10	4,02	5.602.840,10
2005	7.004.180,00	386.556,37	5,52	7.390.736,37
2006	9.452.990,00	323.428,58	3,42	9.776.418,58

GESTIÓN ECONÓMICA

**PRESUPUESTO DE GASTOS COMPARADO POR CAPÍTULOS
OBLIGACIONES RECONOCIDAS**

CAPÍTULO	AÑO 2002	AÑO 2003	AÑO 2004	AÑO 2005	AÑO 2006
GASTOS DE PERSONAL	2.211.348,96	2.353.460,92	2.756.427,69	3.330.708,47	3.662.263,03
GASTOS CORRIENTES	1.721.158,93	1.959.734,32	2.159.855,33	2.968.121,67	4.622.500,14
GASTOS FINANCIEROS	17.310,16	7.933,87	0,00	0,00	44.720,62
INVERSIONES REALES	127.992,99	299.979,65	281.604,45	737.509,23	1.122.812,68
ACTIVOS FINANCIEROS	5.497,46	4.360,11	6.130,00	2.975,73	6.144,11
TOTALES	4.083.308,50	4.625.468,87	5.204.017,47	7.039.315,10	9.458.440,58

GESTIÓN ECONÓMICA

EJECUCIÓN PRESUPUESTARIA 2002
PRESUPUESTO DE GASTOS

CAPÍTULO	CRÉDITOS INICIALES	MODIFICACIONES	CRÉDITOS DEFINITIVOS	OBLIGACIONES RECONOCIDAS	PAGOS REALIZADOS	C. DEFINITIVOS/ O. RECONOCIDAS
GASTOS DE PERSONAL	2.483.940,00	45.955,00	2.529.895,00	2.211.348,96	2.211.348,96	87,41%
GASTOS CORRIENTES	1.610.180,00	246.702,38	1.856.882,38	1.721.158,93	1.706.929,26	92,69%
GASTOS FINANCIEROS	18.060,00		18.060,00	17.310,16	17.310,16	95,85%
INVERSIONES REALES	192.320,00	-31.300,00	161.020,00	127.992,99	127.776,75	79,49%
ACTIVOS FINANCIEROS	6.010,00		6.010,00	5.497,46	5.497,46	91,47%
TOTALES	4.310.510,00	261.357,38	4.571.867,38	4.083.308,50	4.068.862,59	89,31%

EJECUCIÓN PRESUPUESTARIA 2003
PRESUPUESTO DE GASTOS

CAPÍTULO	CRÉDITOS INICIALES	MODIFICACIONES	CRÉDITOS DEFINITIVOS	OBLIGACIONES RECONOCIDAS	PAGOS REALIZADOS	C. DEFINITIVOS/ O. RECONOCIDAS
GASTOS DE PERSONAL	2.585.110,00	17.722,04	2.602.832,04	2.353.460,92	2.342.476,68	90,42%
GASTOS CORRIENTES	1.868.000,00	143.993,63	2.011.993,63	1.959.734,32	1.919.180,39	97,40%
GASTOS FINANCIEROS	18.060,00		18.060,00	7.933,87	7.933,87	43,93%
INVERSIONES REALES	300.000,00		300.000,00	299.979,65	299.594,22	99,99%
ACTIVOS FINANCIEROS	6.010,00		6.010,00	4.360,11	4.360,11	72,55%
TOTALES	4.777.180,00	161.715,67	4.938.895,67	4.625.468,87	4.573.545,27	93,65%

GESTIÓN ECONÓMICA

EJECUCIÓN PRESUPUESTARIA 2004
PRESUPUESTO DE GASTOS

CAPÍTULO	CRÉDITOS INICIALES	MODIFICACIONES	CRÉDITOS DEFINITIVOS	OBLIGACIONES RECONOCIDAS	PAGOS REALIZADOS	C. DEFINITIVOS/ O. RECONOCIDAS
GASTOS DE PERSONAL	3.038.540,00	33.088,94	3.071.628,94	2.756.427,69	2.738.163,09	89,74%
GASTOS CORRIENTES	2.035.840,00	183.241,16	2.219.081,16	2.159.855,33	2.072.845,70	97,33%
GASTOS FINANCIEROS	0,00		0,00	0,00	0,00	
INVERSIONES REALES	306.000,00		306.000,00	281.604,45	277.199,47	92,03%
ACTIVOS FINANCIEROS	6.130,00		6.130,00	6.130,00	6.130,00	100,00%
TOTALES	5.386.510,00	216.330,10	5.602.840,10	5.204.017,47	5.094.338,26	92,88%

EJECUCIÓN PRESUPUESTARIA 2005
PRESUPUESTO DE GASTOS

CAPÍTULO	CRÉDITOS INICIALES	MODIFICACIONES	CRÉDITOS DEFINITIVOS	OBLIGACIONES RECONOCIDAS	PAGOS REALIZADOS	C. DEFINITIVOS/ O. RECONOCIDAS
GASTOS DE PERSONAL	3.682.280,00	-21.643,63	3.660.636,37	3.330.708,47	3.306.917,67	90,99%
GASTOS CORRIENTES	2.797.410,00	171.000,00	2.968.410,00	2.968.121,67	2.810.051,05	99,99%
GASTOS FINANCIEROS	0,00	0,00	0,00	0,00	0,00	
INVERSIONES REALES	518.240,00	237.200,00	755.440,00	737.509,23	546.040,01	97,63%
ACTIVOS FINANCIEROS	6.250,00	0,00	6.250,00	2.975,73	2.975,73	47,61%
TOTALES	7.004.180,00	386.556,37	7.390.736,37	7.039.315,10	6.665.984,46	95,25%

GESTIÓN ECONÓMICA

EJECUCIÓN PRESUPUESTARIA 2006
PRESUPUESTO DE GASTOS

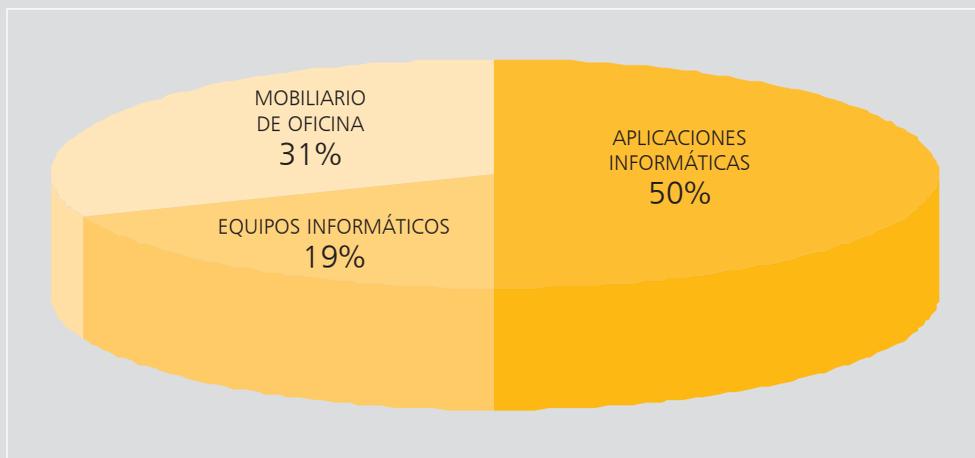
CAPÍTULO	CRÉDITOS INICIALES	MODIFICACIONES	CRÉDITOS DEFINITIVOS	OBLIGACIONES RECONOCIDAS	PAGOS REALIZADOS	C. DEFINITIVOS/ O. RECONOCIDAS
GASTOS DE PERSONAL	4.099.610,00	-203.296,84	3.896.313,16	3.662.263,03	3.640.101,94	93,99%
GASTOS CORRIENTES	4.100.000,00	526.725,42	4.626.725,42	4.622.500,14	4.327.075,03	99,91%
GASTOS FINANCIEROS	122.400,00	0,00	122.400,00	44.720,62	44.720,62	36,54%
INVERSIONES REALES	1.124.600,00	0,00	1.124.600,00	1.122.812,68	1.014.885,45	99,84%
ACTIVOS FINANCIEROS	6.380,00	0,00	6.380,00	6.144,11	6.144,11	96,30%
TOTALES	9.452.990,00	323.428,58	9.776.418,58	9.458.440,58	9.032.927,15	96,75%

GESTIÓN ECONÓMICA

COMPOSICIÓN DEL INMOVILIZADO A 31 DICIEMBRE 2006

	VALOR	AMORTIZACIÓN	VALOR NETO	NÚMERO DE ELEMENTOS
APLICACIONES INFORMÁTICAS	1.705.040,44	891.940,63	813.099,81	135
EQUIPOS INFORMÁTICOS	662.990,24	264.722,52	398.267,72	783
MOBILIARIO DE OFICINA	1.040.659,03	249.445,97	791.213,06	2.071
TOTALES	3.408.689,71	1.406.109,12	2.002.580,59	2.989

DETALLE DEL INMOVILIZADO A 31 DICIEMBRE 2006

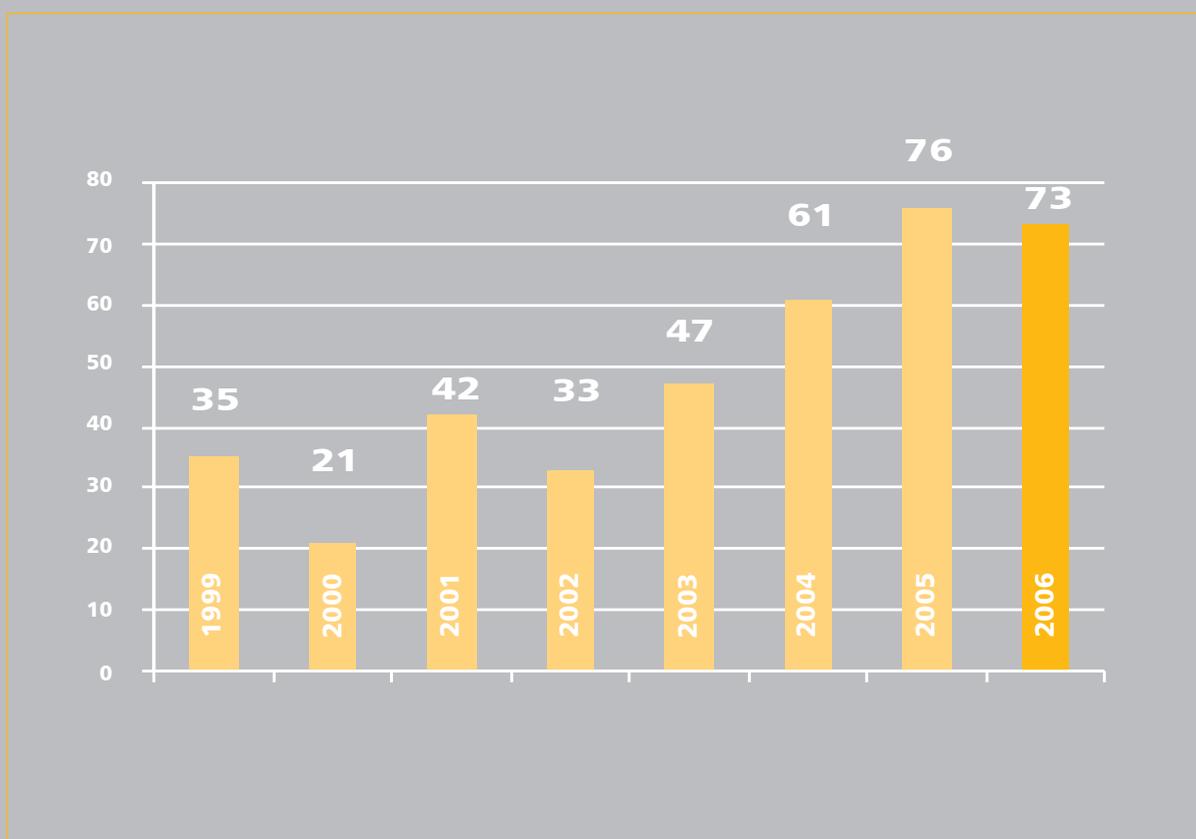


ASISTENCIA A REUNIONES EN EL ÁMBITO INTERNACIONAL DURANTE EL AÑO 2006

COMISIÓN EUROPEA (DG. JUSTICIA Y DERECHOS FUNDAMENTALES)	Sesiones Plenarias Grupo de Trabajo del Artículo 29	5
	Subgrupos:	
	Internet	4
	Cumplimiento y Aplicación de la Legislación (Enforcement)	2
	Asunto Swift	1
	Ley Sarbanes-Oxley	1
	RFID	4
	Datos méritos	3
COMISIÓN EUROPEA (DG. INFO)	Contact Network of Spam Authorities (CNSA)	1
COMISIÓN EUROPEA (DG. AMPLIACIÓN)		1
CONSEJO DE EUROPA		2
CONSEJO DE LA UE	ACC del Convenio de Schengen	5
	ACC del Convenio Europol	5
	ACC Sistema Información Aduanero	1
	ACC Eurojust	1
	ACC Eurodac	1
	Grupo de Trabajo de Policía	2
	Jornadas Convenio Prüm	2
PARLAMENTO EUROPEO		1
OCDE		1
GRUPOS DE TRABAJO SECTORIALES	Grupo de Telecomunicaciones de Berlín	2
	Grupo de Tratamiento de Reclamaciones	2
RELACIONES BILATERALES	Portugal	2
	Bosnia-Herzegovina	2
CONFERENCIAS INTERNACIONALES		3
SEMINARIO UNIVERSIDAD GEORGETOWN		10
TOTAL REUNIONES 2006		64

INFORMES PRECEPTIVOS

EVOLUCIÓN DE INFORMES Y DISPOSICIONES



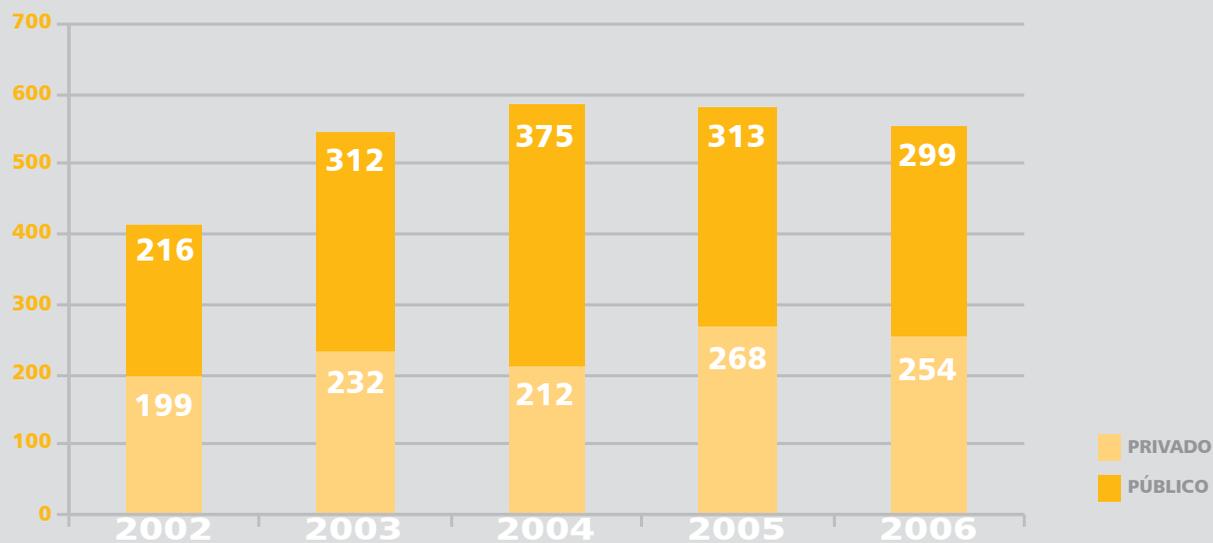
INFORMES PRECEPTIVOS

EVOLUCIÓN DE INFORMES PRECEPTIVOS



CONSULTAS PLANTEADAS

EVOLUCIÓN DE CONSULTAS 2002-2006



DISTRIBUCIÓN DE CONSULTAS 2006

ADMINISTRACIONES PÚBLICAS 254

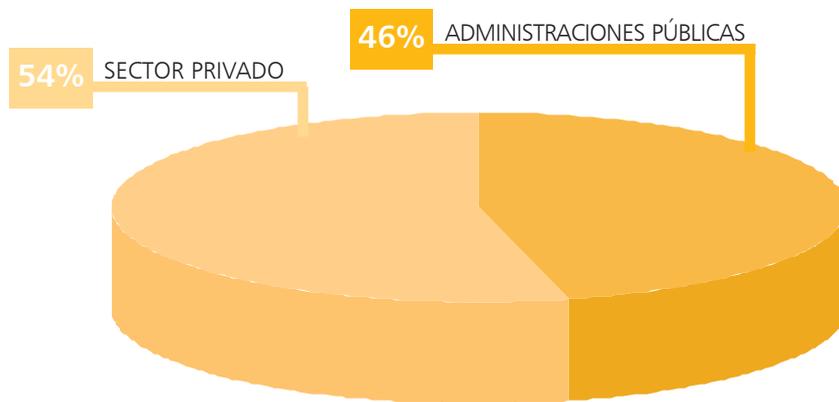
Administración General del Estado	115
Comunidades Autónomas	36
Entidades Locales	66
Otros Organismos Públicos	37

CONSULTAS PRIVADAS 299

Empresas	196
Particulares	58
Asociaciones/Fundaciones	29
Sindicatos	10
Otros	6

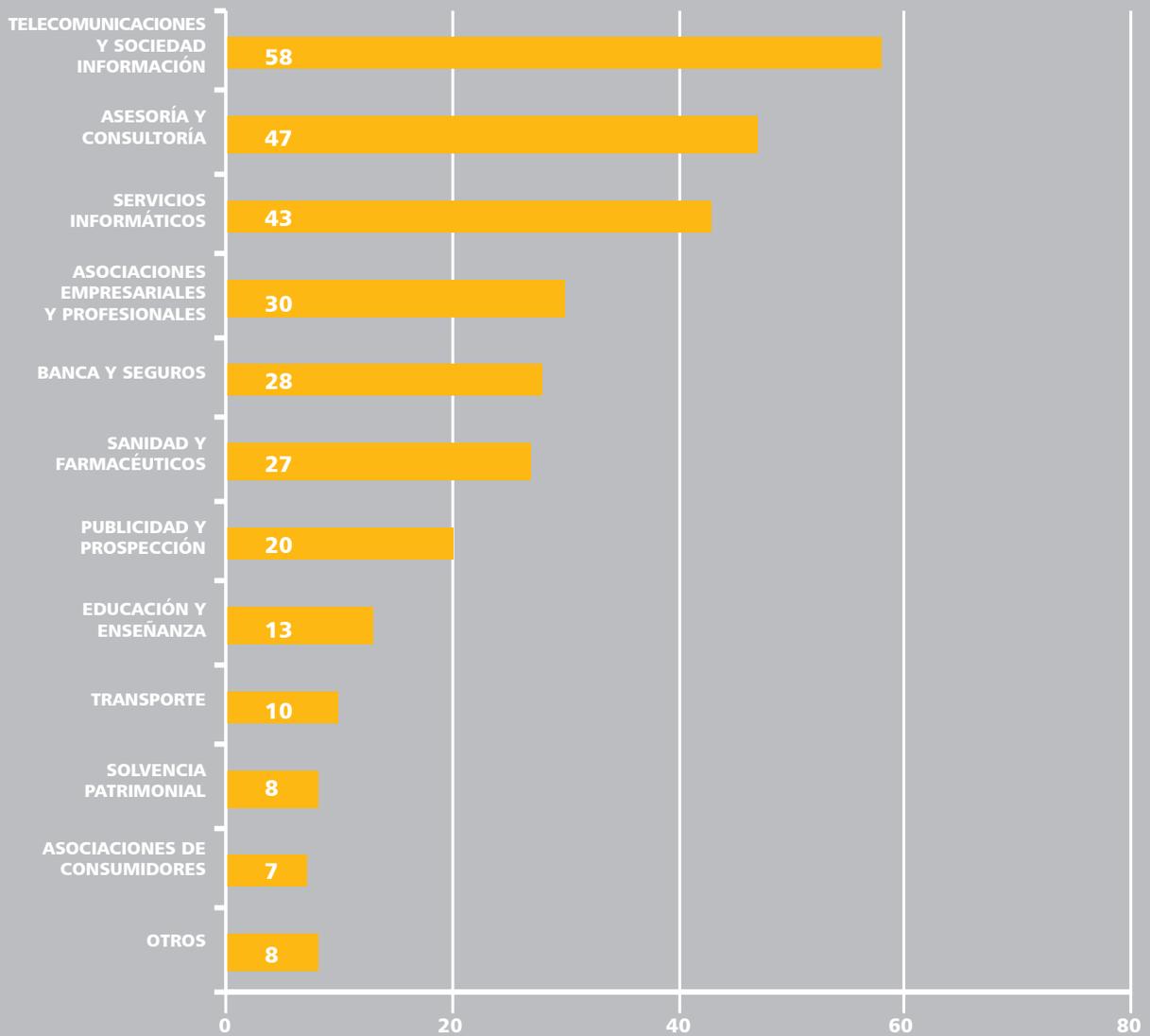
CONSULTAS PLANTEADAS

DISTRIBUCIÓN DE CONSULTAS SECTOR PÚBLICO-SECTOR PRIVADO



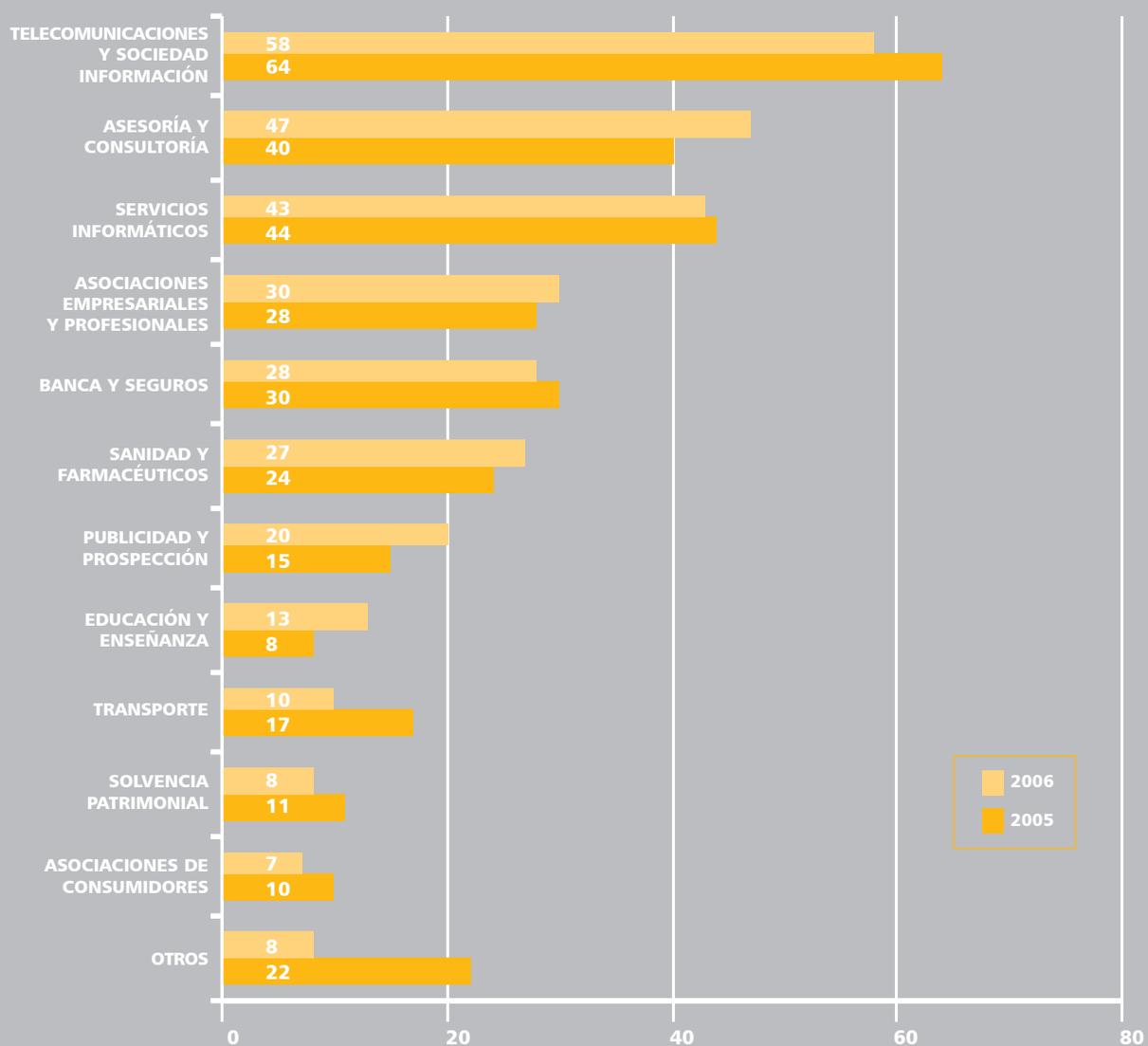
CONSULTAS PLANTEADAS: DISTRIBUCIÓN SECTORIAL

DISTRIBUCIÓN DE LAS CONSULTAS POR SECTORES



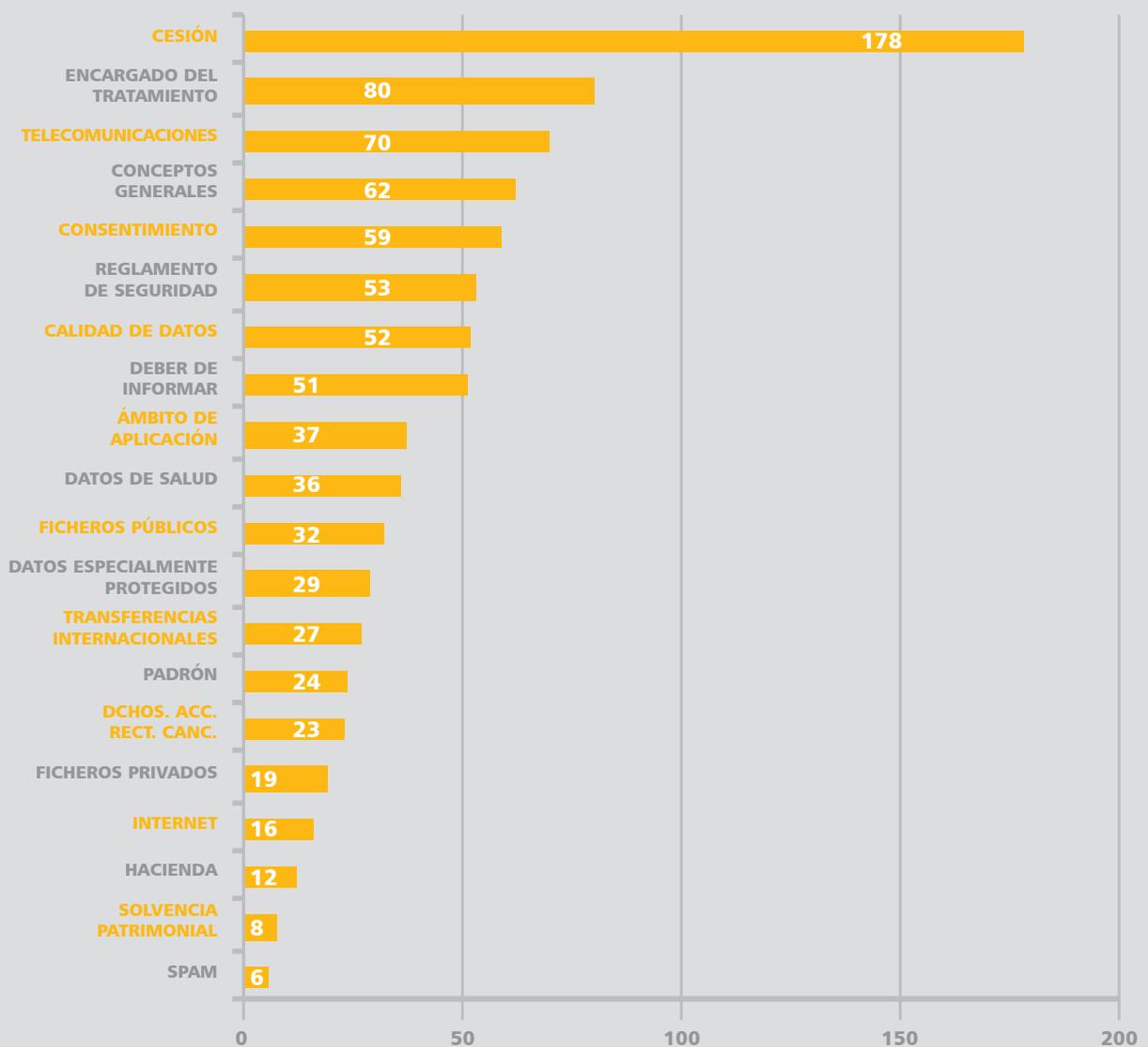
CONSULTAS PLANTEADAS: DISTRIBUCIÓN SECTORIAL

EVOLUCIÓN CONSULTAS POR SECTORES 2005-2006



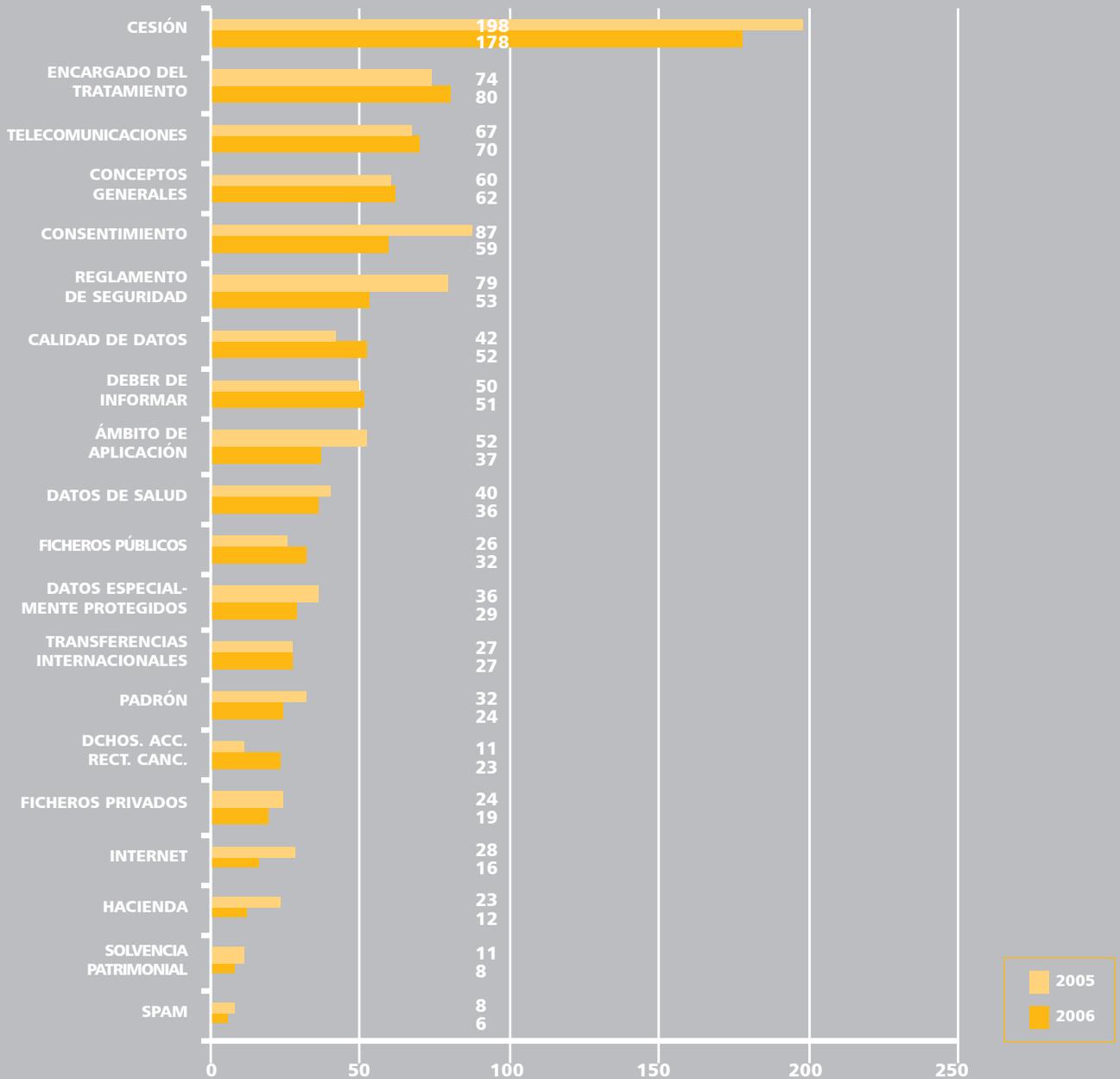
CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

CONSULTAS POR MATERIAS



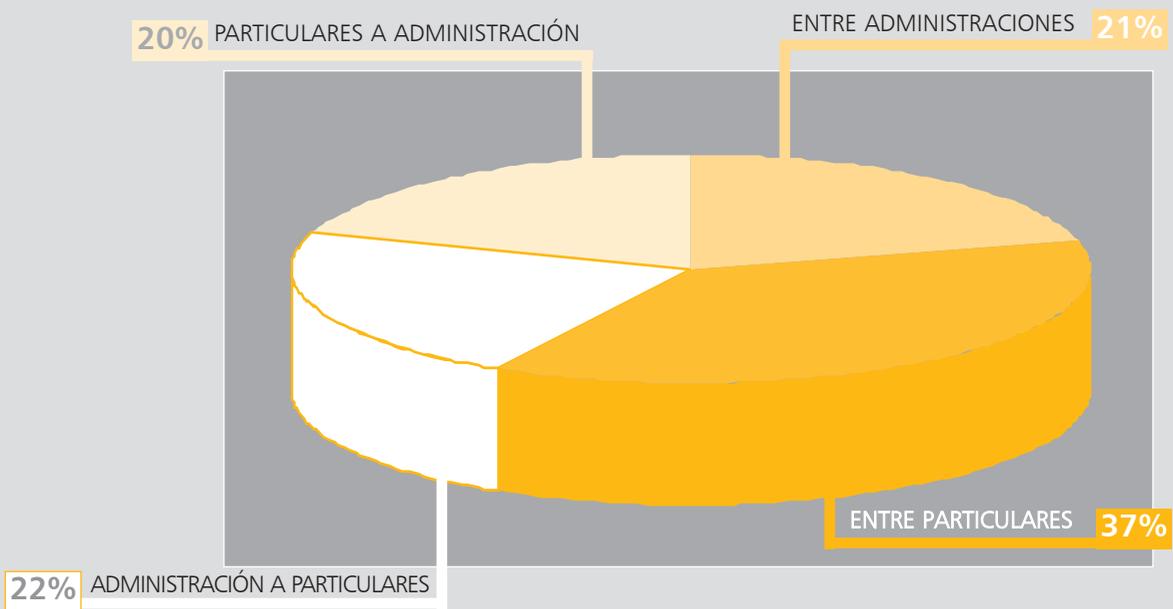
CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS 2005-2006



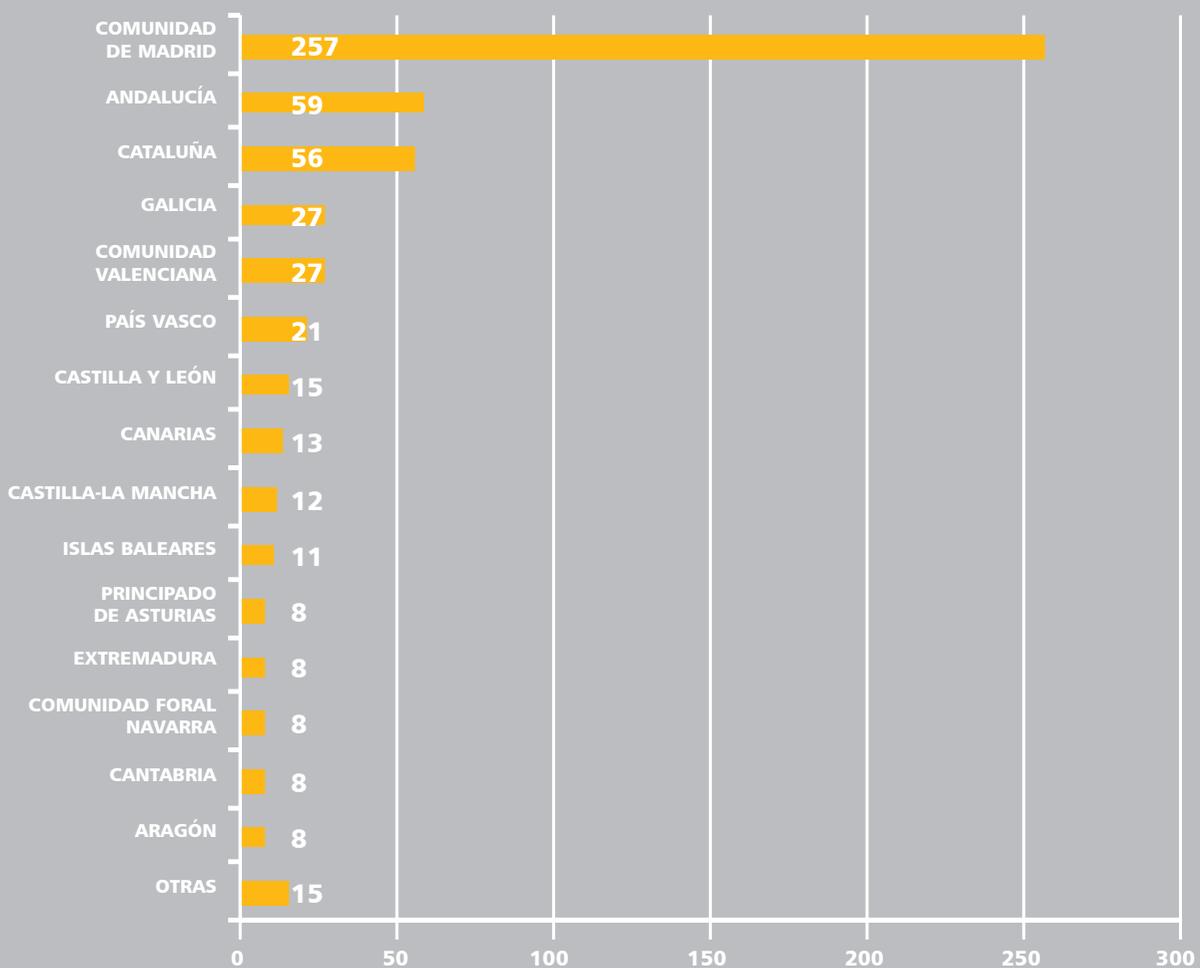
CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

CONSULTAS SOBRE CESIONES DE DATOS



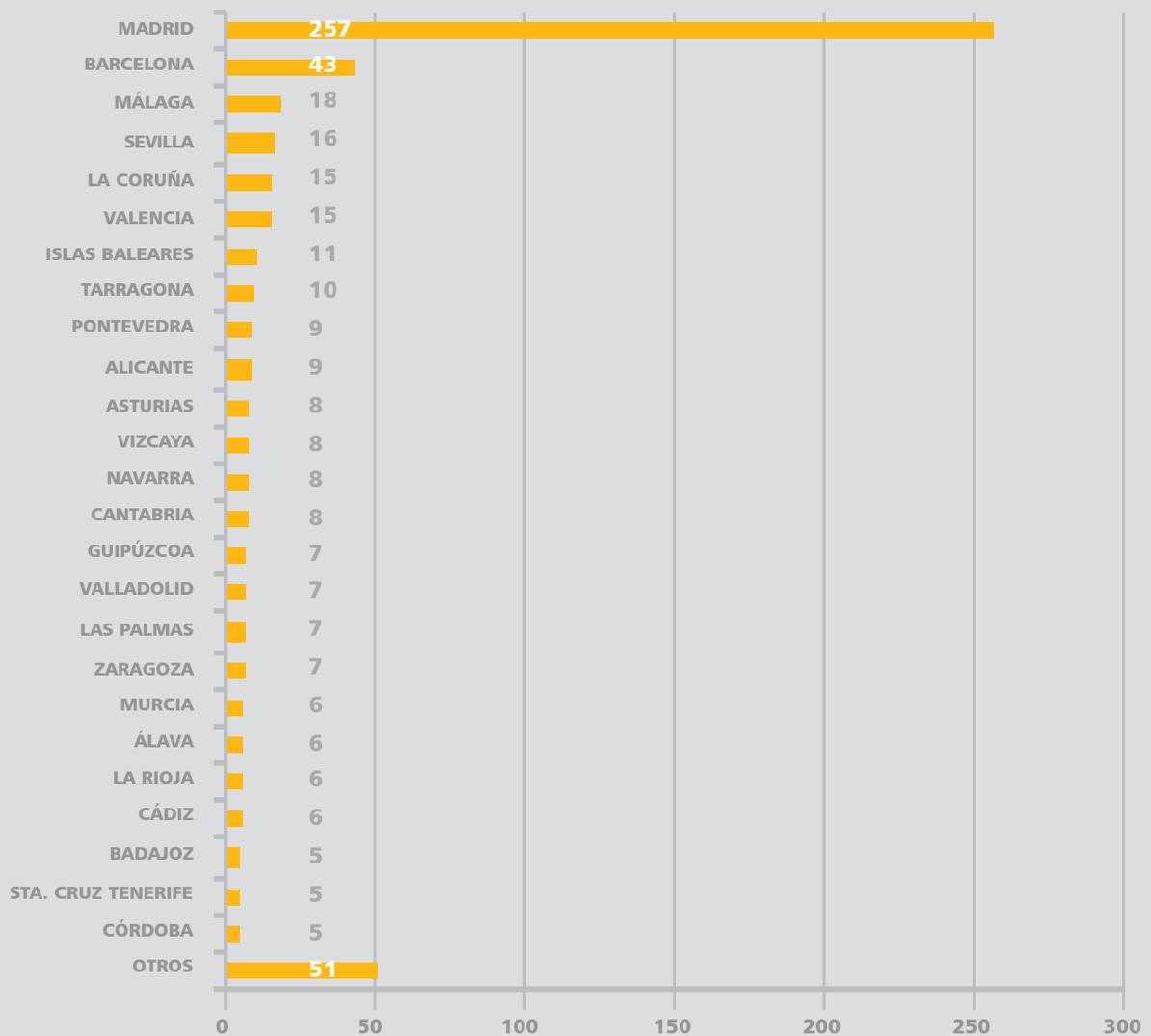
CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

CONSULTAS POR COMUNIDADES AUTÓNOMAS



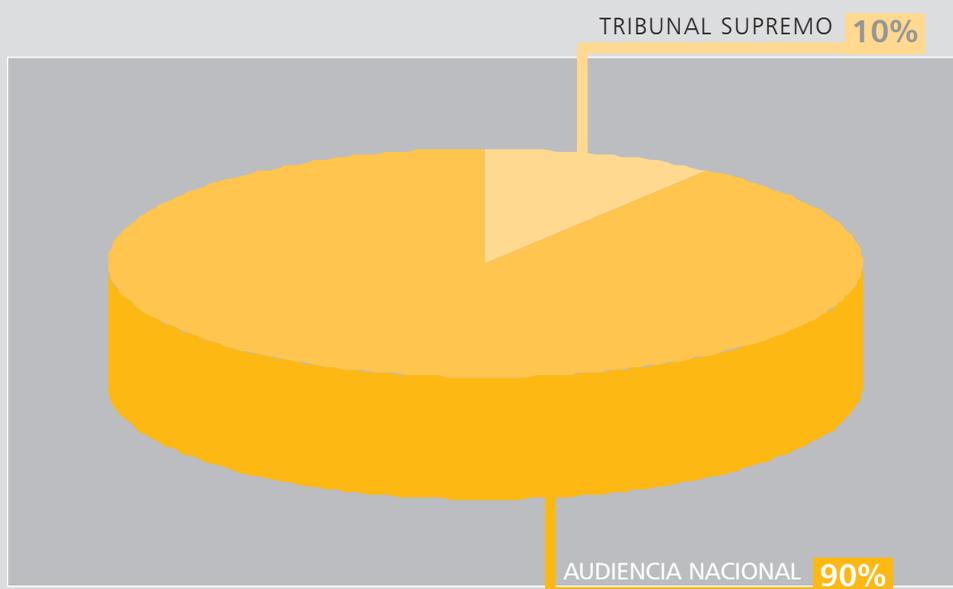
CONSULTAS PLANTEADAS: DISTRIBUCIÓN POR MATERIAS

CONSULTAS POR PROVINCIAS



SENTENCIAS: ÓRGANOS ENJUICIADORES

SENTENCIAS POR ÓRGANO JURISDICCIONAL

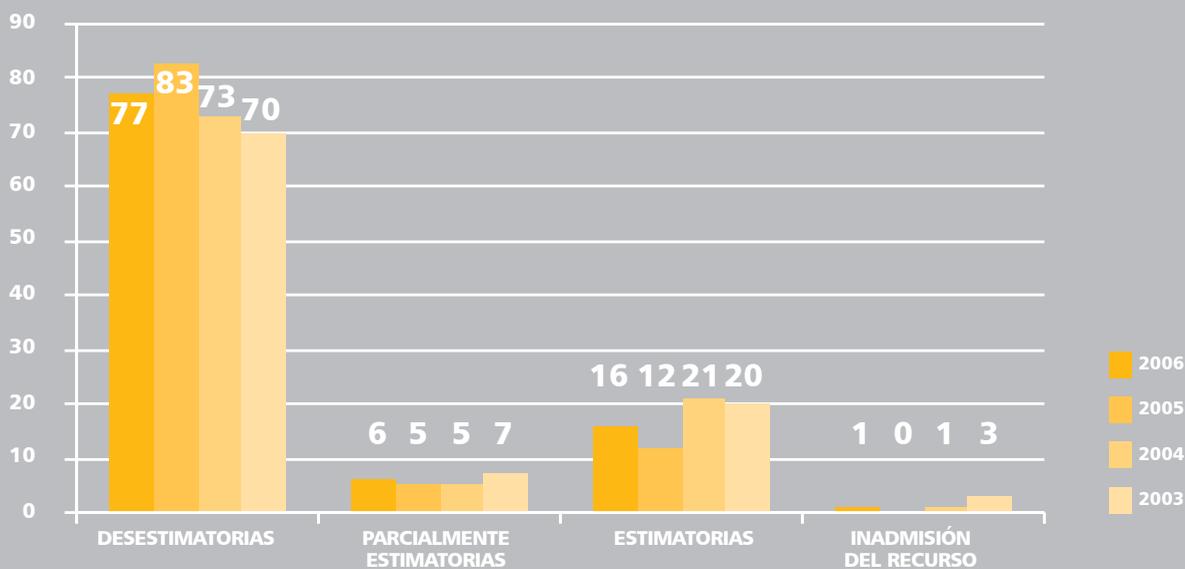


SENTENCIAS: SENTIDO DEL FALLO

SENTENCIAS DE LA AUDIENCIA NACIONAL

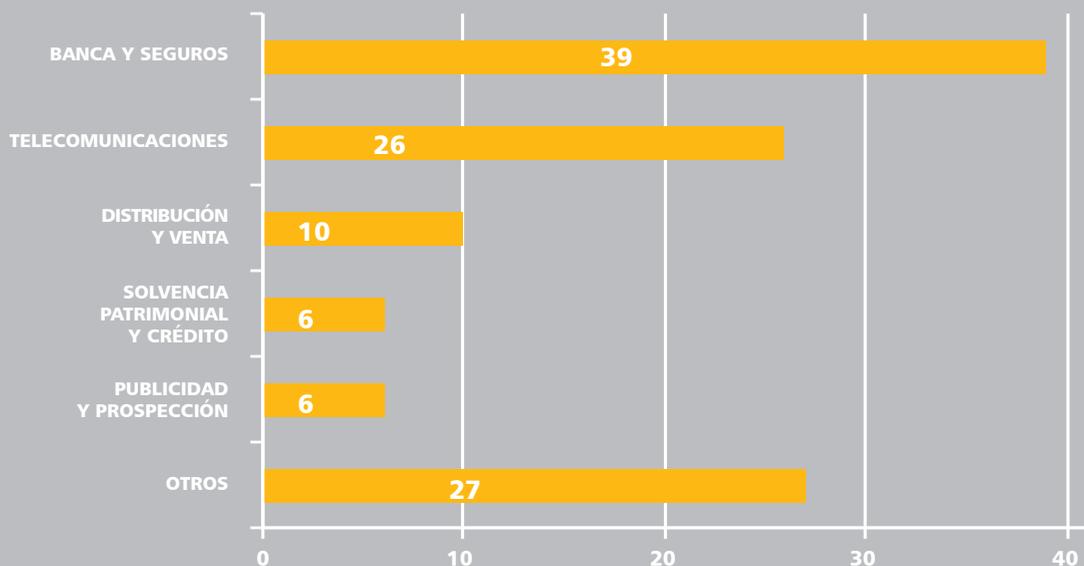


COMPARATIVA SENTENCIAS EN PRIMERA O ÚNICA INSTANCIA PORCENTAJES

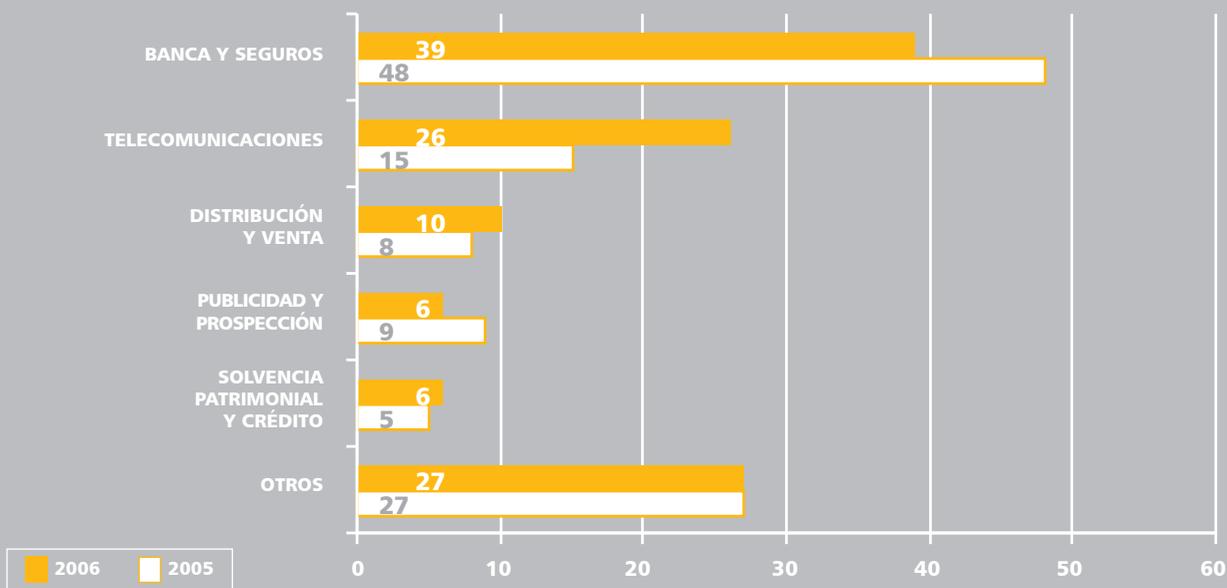


SENTENCIAS: DISTRIBUCIÓN SECTORIAL

SENTENCIAS POR SECTORES

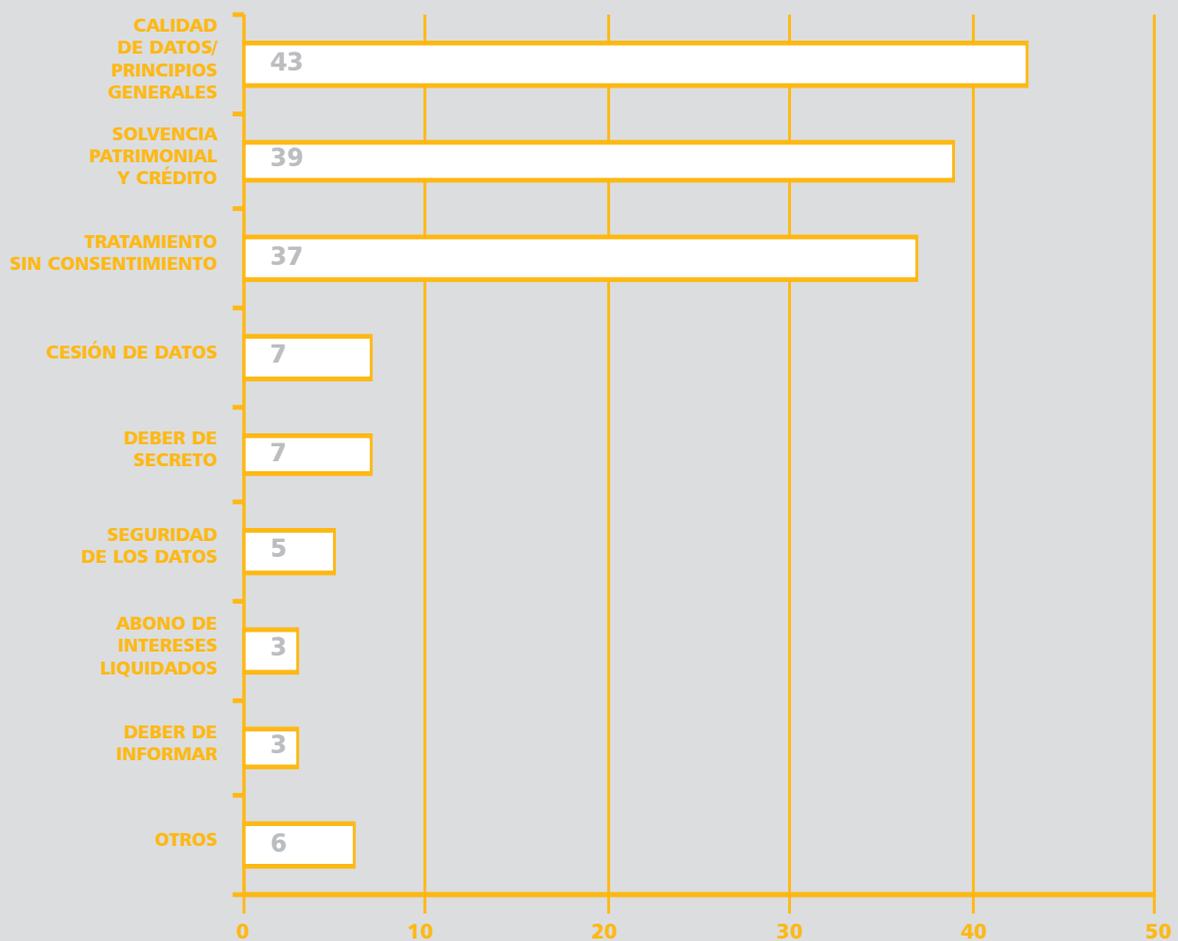


COMPARATIVA POR SECTORES



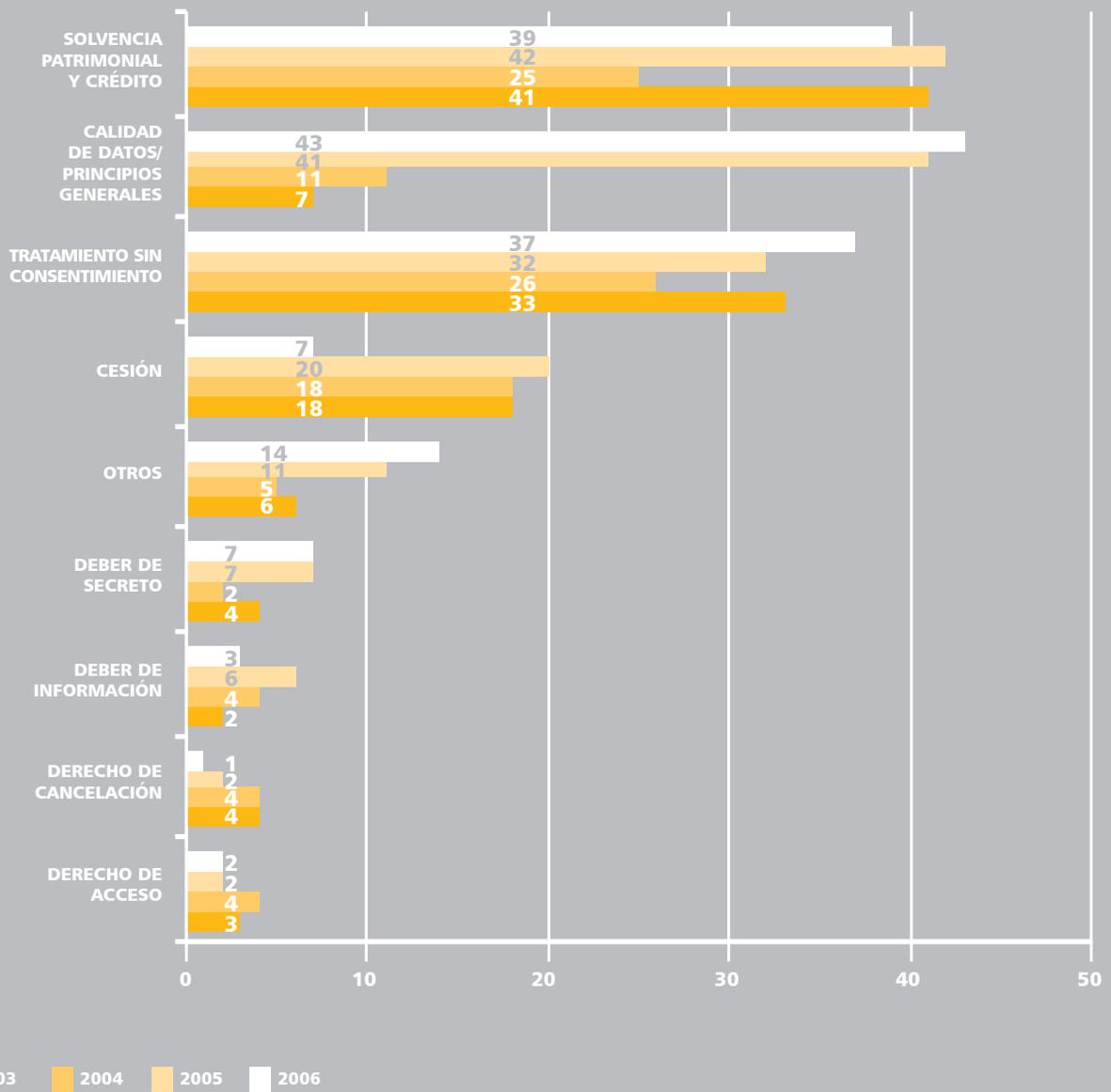
SENTENCIAS: DISTRIBUCIÓN POR MATERIAS

SENTENCIAS POR MATERIAS



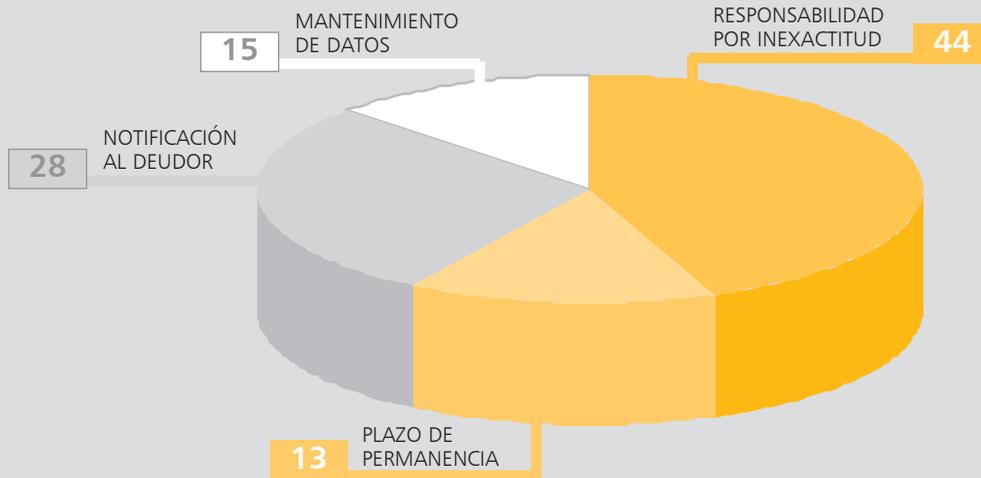
SENTENCIAS: DISTRIBUCIÓN POR MATERIAS

COMPARATIVA POR MATERIAS 2003-2006

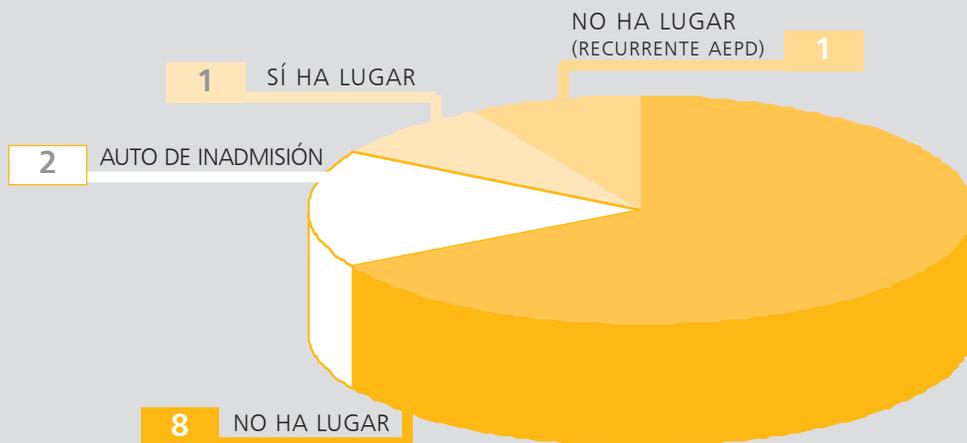


SENTENCIAS: DISTRIBUCIÓN POR MATERIAS

SENTENCIAS SOBRE SOLVENCIA PATRIMONIAL



RESOLUCIONES EN CASACIÓN



Anexo

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**NATURALEZA JURÍDICA**

El art. 35 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), establece que "La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones".

El art. 79 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, publicada el día 31 de diciembre de 2003, ha modificado el nombre de la Agencia de Protección de Datos, por lo que a partir del día 1 de enero de 2004, ha pasado a denominarse Agencia Española de Protección de Datos.

Por su parte el Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la Agencia Española de Protección de Datos (en lo sucesivo EAEPD), que continúa vigente en tanto no sea aprobado otro nuevo, completa la descripción de la naturaleza jurídica que realiza el citado art. 35 de la LOPD, señalando en su art. 1 que se trata de un ente público de los previstos en el art. 6.5 del Real Decreto Legislativo 1091/1988, de 23 de septiembre, que aprueba el Texto Refundido de la Ley General Presupuestaria. Este precepto fue derogado por la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado que, sin embargo, establece en su disposición adicional décima el régimen jurídico de determinados entes públicos, entre los que se encuentra la Agencia Española de Protección de Datos (en lo sucesivo AEPD).

Del marco normativo señalado en el párrafo anterior, se deduce la primera característica que identifica la naturaleza jurídica de la AEPD. Se trata de un ente público que continuará rigiéndose por su legislación específica y, supletoriamente, por la Ley de Organización y Funcionamiento de la Administración General del Estado. En consecuencia se rige por lo establecido en la LOPD, el EAEP y el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD (la disposición transitoria tercera de la LOPD prevé su vigencia en tanto no se oponga a su contenido) y la Resolución de la AEPD, de 30 de mayo de 2000, en lo relativo a los modelos de notificaciones para inscripción de ficheros en el Registro General de Protección de Datos.

Además la Ley 6/1997, al respetar la normativa específica de la AEPD, exceptiona a este ente público, entre otros, del proceso de adaptación que recoge en su disposición transitoria tercera.

El art. 1.2 del EAEPD dispone que la Agencia actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

A la vista de todo lo anterior, cabe concluir que la configuración jurídica de la AEPD se adapta plenamente a las disposiciones que en este sentido se recogen en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y más concretamente a la disposición incluida en su art. 28.1 que establece que "Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva", añadiendo que "Estas autoridades ejercerán las funciones que les son atribuidas con total independencia".

Esta exigencia de independencia se recoge, asimismo, en la Carta Europea de los Derechos Fundamentales, proclamada en Niza el 8 de diciembre de 2000, y que ha sido incorporada a la Parte II del Proyecto de Tratado por el que se instituye una Constitución para Europa, en cuyo artículo 68, dedicado a la protección de los datos de carácter personal (transcrito íntegramente en el capítulo anterior de esta Memoria), se establece que "El respeto de estas normas estará sujeto al control de una autoridad independiente".

La importancia de esta exigencia queda patente si se tiene en cuenta que se reitera expresamente en el Título IV de dicho Tratado, sobre "la Vida Democrática de la Unión" en su artículo 50, relativo a la protección de datos de carácter personal (también transcrito en su totalidad en el anterior capítulo).

A modo de recapitulación, la AEPD es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que se regula por su normativa específica, y que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

RÉGIMEN JURÍDICO APLICABLE

En el apartado anterior, que hemos dedicado a delimitar la peculiar naturaleza jurídica de la AEPD, ha quedado especificado que la misma se regirá, con carácter preferente, por su normativa específica. Pasemos ahora a pormenorizar cual es el régimen jurídico de los diferentes ámbitos de actuación.

El art. 35 de la LOPD va enumerando los diferentes ámbitos de la siguiente manera:

- En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la LOPD y sus disposiciones de desarrollo, actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. De este modo el art. 35.2 de la LOPD, recoge lo establecido en el art. 2.2 de la citada Ley 30/1992, cuando establece que las entidades de derecho público sujetarán su actividad a dicha Ley cuando ejerzan potestades administrativas, sometiéndose en el resto de su actividad a lo que dispongan sus normas de creación.
- En sus adquisiciones patrimoniales y contratación se regirá por el derecho privado. A tal fin el art. 36 del EAEPD establece que los contratos que celebre se regirán por el derecho privado, pero su adjudicación será acordada con respeto de los principios de publicidad y concurrencia.
- En cuanto al personal que presta servicios en la AEPD, de acuerdo con lo dispuesto en el artículo citado, los puestos de trabajo de los órganos y servicios que la integran son desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. De acuerdo con ello, el régimen del personal que presta servicios en la AEPD, será el previsto en la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública y demás disposiciones de desarrollo, cuando se trate de funcionarios públicos, y en el Convenio Único para el personal laboral de la Administración General del Estado, aprobado por Resolución de la Dirección General de Trabajo de 24 de noviembre de 1998, en el caso de personal contratado.
- Desde el punto de vista del Derecho Presupuestario, la AEPD incorpora su presupuesto dentro de los Presupuestos Generales del Estado. Así el art. 48.1, a) de la Ley General Presupuestaria establece que se integran en los mismos la totalidad de ingresos y gastos del resto de entes del sector público estatal a que se refería, hasta la entrada en vigor de la Ley de Organización y Funcionamiento de la Administración General del Estado, el art. 6.5 que, como ya hemos visto, era el caso de la AEPD.
- Dentro de la Ley de Presupuestos Generales del Estado, la AEPD es el órgano responsable de ejecutar el Programa Presupuestario 146-B "Protección de Datos de Carácter Personal", para lo cual dispone de créditos dentro de la Sección Presupuestaria 13, Organismo Público 301.

Así mismo, en lo relativo al control de las actividades económicas y financieras de la Agencia hay que distinguir entre el control externo que ejerce el Tribunal de Cuentas y el control interno que realiza la Intervención General de la Administración del Estado. En relación con este último, el art. 33.3 del EAEPD dispone que se ejercerá, de conformidad con lo dispuesto en el art. 17.1 de la Ley General Presupuestaria, con carácter permanente. Precisamente en relación con este asunto, el art. 99.3 de esta última Ley señala que los entes públicos, a que se refiere la disposición adicional décima de la Ley de Organización y Funcionamiento de la Administración General del Estado, es decir la que incluye a la AEPD, estarán sometidos al sistema de control de su gestión económico-

financiera establecido en su Ley reguladora, y, en su defecto, al establecido para las entidades públicas empresariales.

Por lo tanto, de acuerdo con lo señalado con anterioridad, la AEPD está sometida a control financiero permanente. Esto quiere decir que dicho control se ejerce por una Intervención Delegada, sin perjuicio de las actuaciones que a nivel central ejerce la propia Intervención General de la Administración del Estado. Dicho control financiero permanente se desarrolla de acuerdo con lo dispuesto en el Real Decreto 2188/1995, de 28 de diciembre, por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Administración del Estado, y en las Circulares de dicha Intervención General 1/1989, de 2 de enero, 2/1989, de 28 de abril, y 5/1992, de 14 de diciembre.

En lo relativo al control externo que ejerce el Tribunal de Cuentas, a tenor de la Orden Ministerial de 1 de febrero de 1996, por la que se aprueba la Instrucción de Contabilidad para la Administración Institucional, se realiza por medio del informe de auditoría que efectúa la Intervención General de la Administración del Estado y acaba siendo remitido al citado Tribunal.

La contabilidad de la Agencia se ajusta al Plan General de Contabilidad Pública, aprobado por Orden Ministerial de 6 de mayo de 1994. A tenor de dicho Plan, la AEPD ha de elaborar sus cuentas anuales (Balance, Cuenta de Resultado Económico - Patrimonial, Estado de Liquidación del Presupuesto y Memoria), sobre las cuales la Intervención General de la Administración del Estado realiza un informe de auditoría antes de remitirlas al Tribunal de Cuentas. Finalmente, se publica en el Boletín Oficial del Estado un resumen de las cuentas anuales, a tenor de lo previsto en la Orden del Ministerio de Hacienda de 28 de junio de 2000.

ESTRUCTURA Y FUNCIONES

CARÁCTER DE AUTORIDAD INDEPENDIENTE

Antes de entrar a analizar la estructura orgánica básica de la AEPD, resulta capital recordar lo dispuesto en el art. 35.1 de la LOPD, ya que en él se reconoce el carácter de entidad independiente de la propia Agencia. Efectivamente, tal y como se ha indicado, el citado precepto señala lo siguiente:

"La Agencia Española de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno".

A mayor abundamiento, el art. 1.2 del EAEPD dispone que:

"La Agencia Española de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia".

ESTRUCTURA ORGÁNICA

La estructura orgánica básica de la AEPD se establece en el art. 11 de su Estatuto, que distingue los siguientes órganos:

- El Director.
- El Consejo Consultivo.
- El Registro General de Protección de Datos, en lo sucesivo RGPD.
- La Inspección de Datos, en lo sucesivo SGID.
- La Secretaría General, en lo sucesivo SGAEPD.

Además, para el ejercicio de sus funciones el Director de la AEPD es asistido por una Unidad de Apoyo integrada por el Adjunto al Director el Vocal asesor-jefe de Gabinete y el Gabinete Jurídico. Ésta Unidad realiza, entre otras funciones, las de asesoramiento jurídico, interpretación normativa, emisión de informes, e impulso y desarrollo de las relaciones internacionales de la Agencia.

EL DIRECTOR

A tenor del art. 36 de la LOPD, dirige la Agencia y ostenta la representación de la misma, ejerce sus funciones con plena independencia y objetividad. El Director de la AEPD, con rango de Subsecretario, desempeña su cargo con dedicación absoluta, plena independencia y total objetividad. No estará sujeto a instrucción de autoridad alguna. Deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

En el EAEPD se distingue entre las funciones de dirección (art. 12) y las funciones de gestión que corresponden al Director de la Agencia, de la siguiente manera:

- Funciones de dirección en las que el Director dictará las resoluciones e instrucciones que se requieran en relación con las competencias que corresponden a la Agencia. Dentro de ellas, destacan las referentes a procedencia o improcedencia de las inscripciones en el RGPD, requerimientos a los responsables de los ficheros de titularidad privada para que subsanen deficiencias de los códigos-tipo, procedencia o

improcedencia de la denegación del acceso a algunos ficheros automatizados, autorización o denegación de transferencias internacionales de datos a países con un nivel de protección no adecuado, adopción de medidas cautelares y acuerdos de iniciación en relación con el ejercicio de la potestad sancionadora respecto a responsables de ficheros privados, solicitud de incoación de expedientes disciplinarios contra los responsables de ficheros públicos, y autorización de entrada en los locales en que se hallen los ficheros con el fin de proceder a las inspecciones que sean pertinentes.

- Funciones de gestión en las que el Director actúa en relación con la ejecución de la actividad económico-financiera de la Agencia. A tal fin adjudica, formaliza y controla el seguimiento de los contratos de la Agencia, aprueba los gastos y ordena los pagos, ejerce el control económico-financiero de la Agencia, programa su gestión, elabora el anteproyecto de presupuesto, propone la relación de puestos de trabajo, aprueba la Memoria Anual de la Agencia y ordena la convocatoria de las reuniones del Consejo Consultivo. En relación con estas funciones el Director podrá delegar en el Secretario General todas ellas, salvo las que se refieren al control económico-financiero de la Agencia, a la aprobación de la Memoria Anual, y a la ordenación de las convocatorias del Consejo Consultivo. Por Resolución del Director de la AEPD de 16 de febrero de 2004 (B.O.E. de 2 de marzo) se delegaron en el Secretario General diversas competencias.

Por su parte, el art. 37 de la LOPD confía a la AEPD otras funciones que se refieren al cumplimiento de la legislación sobre protección de datos, a la adecuación de los tratamientos a los principios de la ley y al informe preceptivo de los proyectos de disposiciones generales que desarrollen el contenido de la LOPD.

El EAEPD, detalla las funciones de la Agencia en su capítulo II, distinguiendo entre las referentes a las relaciones con los afectados, las de cooperación en la elaboración y aplicación de las normas, las relativas a los ficheros estadísticos, la publicidad de los ficheros, la elaboración de una memoria anual y las relaciones internacionales.

Por lo que se refiere a las relaciones con los afectados, el art. 37 de la LOPD y el Estatuto atribuyen a la Agencia la función de informar a las personas de los derechos que la Ley les reconoce en esta materia, pudiendo promover, a tal efecto, campañas de difusión, valiéndose de los medios de comunicación social, así como atender las peticiones y reclamaciones formuladas por las personas afectadas.

En cuanto a la cooperación en la elaboración y aplicación de las normas, la LOPD, en el precepto citado, y el Estatuto atribuyen a la Agencia la función de informar preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica, así como de cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la misma; las de dictar instrucciones y recomendaciones para adecuar los tratamientos a los principios de la Ley y las de dictar recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de datos y control de acceso a los ficheros.

En lo que respecta a los ficheros estadísticos, el art. 37 de la LOPD y el Estatuto atribuyen a la Agencia la función de velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el art. 46 de la LOPD, relativo a las infracciones de las Administraciones Públicas.

Por lo que se refiere a la publicidad de los ficheros, la LOPD y el Estatuto encomiendan a la Agencia la función de velar por la publicidad de la existencia de los ficheros de datos de carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la misma determine.

Por otra parte, el citado art. 37 de la LOPD y el EAEPD encomiendan a la Agencia la redacción de una memoria anual y su remisión al Ministerio de Justicia, para su ulterior envío a las Cortes Generales. Esta memoria, de acuerdo con dicho Estatuto, además de la información necesaria sobre el funcionamiento de la Agencia, comprenderá los siguientes aspectos: una relación de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos; un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos; un análisis y una valoración de los problemas de la protección de datos a escala nacional.

Por lo que se refiere a las relaciones internacionales, el referido art. 37 de la LOPD y el EAEPD (modificado en este punto por el Real Decreto 156/1996, de 2 de febrero) atribuyen a la Agencia las funciones de cooperación internacional en materia de protección de datos personales. En este ámbito, se dispone que la Agencia prestará asistencia a las autoridades designadas por los Estados parte en el Convenio del Consejo de Europa de 28 de enero de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos previstos en el artículo 13 del Convenio y se designa a la Agencia, como representante español a los efectos previstos en el art. 29 de la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, correspondiendo al Director de la Agencia, la designación de un representante para el Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales, previsto en la disposición citada.

Asímismo dispone el Estatuto que la Agencia ejercerá el control de los datos de carácter personal introducidos en la parte nacional española, de la base de datos del Sistema de Información de Schengen (SIS), correspondiendo al Director, la designación de dos representantes para la autoridad de control común de protección de datos del citado SIS.

Finalmente, la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, ha introducido algunas modificaciones en el régimen de la Agencia Española de Protección de Datos. Concretamente, el art. 82 ha introducido modificaciones en el art. 37 de la LOPD, lo que supuso, como ya se ha indicado en el capítulo anterior, que a partir del 1 de enero de 2004, las resoluciones de la Agencia Española

de Protección de Datos debían hacerse públicas, una vez hubieran sido notificadas a los interesados. La Agencia, a través de la Instrucción 1/2004, de 22 de diciembre, ya aludida, ha regulado la forma y los plazos en que ha de realizarse esta publicación.

EL CONSEJO CONSULTIVO

El Consejo Consultivo es el Órgano colegiado de asesoramiento del Director de la AEPD. A él le corresponde la función de emitir informe en relación con todas las cuestiones que le someta el Director, y podrá formular propuestas sobre temas relacionados con las materias de competencia de la AEPD.

Los miembros del Consejo serán propuestos de la siguiente forma:

- Un vocal por el Congreso de los Diputados.
- Un vocal por el Senado.
- Un vocal de la Administración General del Estado propuesto por el Ministro de Justicia.
- Un vocal de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos.
- Un vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias.
- Un vocal por la Real Academia de la Historia.
- Un vocal por el Consejo de Universidades.
- Un vocal de los usuarios y consumidores propuesto por el Consejo de Consumidores y Usuarios.
- Un vocal del sector de ficheros privados propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

Actúa como Presidente del Consejo Consultivo el Director de la AEPD y como Secretario, con voz y sin voto, el Secretario General de la Agencia.

El Consejo Consultivo se reunirá cuando así lo decida el Director de la AEPD, que, en todo caso, lo convocará una vez cada seis meses. También se reunirá cuando así lo solicite la mayoría de sus miembros.

EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

El Registro General de Protección de Datos es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de acceso, rectificación, oposición y cancelación, regulados en los artículos 14 a 16 de la LOPD.

Corresponde al Registro General de Protección de Datos:

- Instruir los expedientes de inscripción.
- Expedir certificaciones de los asientos.
- Publicar una relación anual de los ficheros notificados e inscritos.

De conformidad con el artículo 39 de la citada Ley serán objeto de inscripción en el Registro:

- Los ficheros de que sean titulares las Administraciones Públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internacionales.
- Los códigos tipo.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El contenido de la inscripción está regulado en el artículo 20 de la LOPD, para los ficheros de titularidad pública y en el artículo 26 para los ficheros de titularidad privada.

Además, por vía reglamentaria se ha regulado el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

En concreto, estos aspectos se encuentran regulados por las siguientes disposiciones:

El Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la LORTAD, y que continúa vigente a tenor de lo dispuesto en la disposición transitoria tercera de la LOPD.

La Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos (sistema NOTA) a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos.

En el Registro quedan inscritas todas las vicisitudes por las que ha pasado la inscripción de un fichero, con la posibilidad de consulta automatizada al histórico.

Los principios de la inscripción de ficheros se pueden resumir en los siguientes puntos:

- El responsable del fichero deberá efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos.
- La inscripción de un fichero de datos es declarativa, es decir, no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la LOPD.
- La notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.
- La notificación de los ficheros al Registro supone, una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quienes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.

LA INSPECCIÓN DE DATOS

La Subdirección General de Inspección de Datos es el órgano de la Agencia Española de Protección de Datos al que, bajo la dirección y superior autoridad del Director, le corresponde desempeñar dos de las más importantes funciones para el efectivo cumplimiento de la LOPD: la función inspectora o investigadora y la función instructora de los expedientes sancionadores y procedimientos de tutela de derechos.

■ FUNCIÓN INSPECTORA

La Inspección de Datos no está contemplada por la LOPD desde la vertiente orgánica, sino sólo desde la funcional, siendo el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la AEPD, el que prevé que las funciones inherentes al ejercicio de la potestad de inspección que el art. 40 de la LOPD atribuye a la Agencia, se ejerzan por un órgano específico y separado de los demás al frente del cual se sitúa a un funcionario con categoría de Subdirector General.

No añade el Estatuto nuevas precisiones sobre el estatuto personal de quienes se encuadran en este órgano a las ya contenidas en la LOPD, la cual dispone que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus cometidos (art. 40), de donde resulta que la inspec-

ción deberá ser desempeñada por funcionarios de carrera. El carácter de "autoridad pública" que el art. 40.2 LOPD atribuye a los Inspectores de Datos significa que las personas responsables de los ficheros y/o tratamientos que ofrezcan resistencia o cometan atentado contra dichos funcionarios/inspectores, podrían incurrir en su caso en responsabilidad penal, exigible conforme a la legislación penal, y en todo caso incurrirían en la responsabilidad administrativa prevista en el art. 44.3.j) de la LOPD, calificada como obstrucción al ejercicio de la función inspectora.

El Estatuto desarrolla el contenido de la potestad de inspección atribuida a la Agencia en el ya citado art. 40 de la LOPD, precisando la facultad de la Inspección de Datos para efectuar inspecciones de oficio, aunque pudieran tener su origen en una denuncia de las personas afectadas, y detallando el alcance concreto de su capacidad para requerir y obtener información, así como examinar in situ los ficheros y sistemas informáticos en los que se traten datos de carácter personal. En conjunto, se trata de una serie de facultades cuya finalidad es la de obtener información y, en su caso, pruebas sobre posibles incumplimientos de la LOPD, que permitan posteriormente al órgano decisorio incoar procedimientos sancionadores y adoptar, en su caso, las medidas pertinentes dirigidas a la cesación de actividades ilícitas en los términos previstos en los arts. 37.f) y 49 de dicha Ley.

Como lógico correlato de esta función inspectora, se impone a los funcionarios que la ejercen el deber de guardar secreto sobre las informaciones que conozcan en el ejercicio de tal función, incluso después de haber cesado en la misma (art. 40.2 in fine); deber cuyo incumplimiento generaría la oportuna responsabilidad disciplinaria mientras se conserve la relación de servicio con la AEPD, y que se reputaría infracción administrativa grave, una vez extinguida dicha relación, al amparo del art. 44.3 g) de la LOPD.

■ FUNCIÓN INSTRUCTORA

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, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones, estructurándose

como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución, correspondiendo al funcionario instructor el desarrollo completo de la fase de Instrucción u Ordenación del procedimiento y la propuesta razonada al Director de la Agencia de las otras dos, es decir, del acuerdo de inicio del procedimiento sancionador y de la Resolución del mismo.

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 actúa 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).

SECRETARÍA GENERAL

A la Secretaría General, de acuerdo con lo dispuesto en los arts. 30 y 31 del EAEPD, le corresponden las siguientes funciones:

- Funciones de apoyo y ejecución: Elaborar los informes y propuestas que les solicite el Director, notificar las resoluciones del Director, ejercer la secretaría del Consejo Consultivo, gestionar los medios personales y materiales, así como atender la gestión económico-administrativa de la AEPD, llevar el inventario, y cuantos asuntos no estén atribuidos a otros órganos de la misma.
- Otras funciones: Formar y actualizar el fondo de documentación en materia de protección de datos, editar los repertorios oficiales de ficheros inscritos en el RGPD, las memorias anuales y cualesquiera otras publicaciones de la AEPD, organizar confe-

rencias, seminarios y cualesquiera otras actividades de cooperación internacional e interregional sobre protección de datos y facilitar la información necesaria para llevar a cabo campañas de difusión a través de los medios de comunicación.

En definitiva corresponde a la Secretaria General, la gestión y administración de los servicios comunes de la Agencia. Entre sus funciones cabe destacar:

■ GESTIÓN DE LOS RECURSOS HUMANOS

Desde la unidad de recursos humanos se gestiona las políticas de personal de la Agencia, no solo la tramitación de concursos y otras formas de provisión de puestos de trabajo para la cobertura de vacantes sino también las funciones relacionadas con las políticas de formación a través de los planes de formación interna y externa del personal, las gestión de la acción social, el plan de pensiones y la implementación de las medidas de prevención de riesgos laborales, en su vertiente de seguridad en el trabajo, higiene industrial, ergonomía y Psicología aplicada así como medicina en el trabajo.

También, desde la unidad de recursos humanos se asumen las relaciones y coordinación con la representación sindical y la junta de personal, de conformidad con lo establecido en la Ley 11/1985 de libertad sindical y la ley 9/1987 de órganos de representación, determinación de las condiciones de trabajo y participación del personal al servicio de las Administraciones Públicas.

■ GESTIÓN DE LOS MEDIOS ECONÓMICOS, MATERIALES E INFORMÁTICOS

La Secretaria a través del servicio de Gestión Económica y Presupuestaria y del Servicio de Informática, provee a la Agencia de los medios materiales para un correcto cumplimiento de las funciones que le son propias. Desde el servicio de Gestión Económica y Presupuestaria se gestiona no solo el presupuesto y la ejecución del gasto sino también la gestión y recaudación de los ingresos tanto en vía voluntaria proveniente de las sanciones pagadas por los infractores como por la vía de apremio, mediante el procedimiento de apremio recogido en el Reglamento General de Recaudación aprobado por RD 939/2005 de 29 de julio. También desde esta unidad se asume la gestión del régimen interior y la llevanza del inventario. Por lo que respecta al Servicio de Informática se encarga del mantenimiento, renovación y mejora de los sistemas, procesos y aplicaciones informáticas y telefónicas de la Agencia, dando soporte al personal y desarrollando y diseñando Los programas específicos necesarios.

■ SERVICIO DE ATENCIÓN AL CIUDADANO

Conforme a lo que establece el artículo 4 del RD 428/1993, por el que se aprueba el estatuto de la Agencia corresponde al Área de Atención al Ciudadano la de informar a los ciudadanos de los derechos que la ley les reconoce en relación con el tratamiento de sus datos personales. Así mismo, atiende las peticiones que les dirigen los afectados

y resuelve las reclamaciones formuladas por éstos. De este modo a la ventanilla de atención al ciudadano acuden tanto ciudadanos particulares preocupados por el uso o abuso de sus datos personales por terceros, como personas jurídicas que desean obtener información sobre sus derechos y obligaciones, como las propias Administraciones Públicas. La labor del Servicio de Atención al ciudadano se realiza mediante la consulta telefónica en el teléfono 901-100-099 o la consulta presencial en la sede de la Agencia Española de protección de Datos en la C/ Jorge Juan nº 6 y a través del buzón de ciudadano al que se puede acceder a través de la página Web [www. agpd. es](http://www.agpd.es)

Además de lo anterior la Secretaria General en virtud de la Resolución de 16 de febrero de 2004 (BOE de 2 de marzo) asume las competencias delegadas del Director de la Agencia en especial la de notificación de sus actos y resoluciones.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



