AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA 2009

Como cada año me llena de satisfacción poder presentar la memoria anual de la Agencia Española de Protección de Datos y, con ello, poder ofrecer una visión integral sobre el estado de situación de la protección de datos en nuestro país.

Esta institución siempre ha valorado enormemente la publicación de este documento por suponer una forma de dar a conocer tanto a instituciones públicas como privadas y, en general, a los ciudadanos la forma en la que se materializa la tutela del derecho fundamental a la protección de datos, Y con ello, el mejor modo de expresar nuestro compromiso con la labor que tenemos encomendada.

La Memoria 2009 incorpora la información más destacada y ofrece un análisis de los principales indicadores que permiten evaluar el nivel de implantación de la normativa de protección de datos, además del alcance de las tensiones y retos a que está sometido, hoy, el derecho fundamental a la protección de datos; principalmente, en relación con el trepidante ritmo de la revolución tecnológica y, en particular, con el desarrollo de servicios con un gran impacto en la privacidad de los ciudadanos.

Asimismo, a lo largo de las próximas páginas los lectores podrán apreciar como los diferentes proyectos e iniciativas puestos en marcha por la institución en los últimos años han permitido la existencia de una mayor concienciación social respecto a la protección de datos de carácter personal. Así lo ponen de relieve, no solo el notable incremento del ejercicio de las funciones que tiene encomendadas la AEPD, sino, también, estudios demoscópicos que, como el barómetro del Centro de Investigaciones Sociológicas (CIS), muestran que en los ciudadanos existe una creciente preocupación por la protección de datos y el uso de su información personal.

La Memoria dedica un apartado específico a la actividad internacional desarrollada por la institución, y a algunas de las novedades más destacadas en el marco normativo europeo que, como el Tratado de Lisboa, han incidido de manera directa en la materia que nos ocupa. Mención especial merecen, por su trascendencia, las referencias contenidas en la memora relativas a la celebración, en noviembre de 2009, en Madrid, del mayor foro dedicado a la privacidad a nivel mundial, la *"31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad"*, y la aprobación de la *"Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad"*.

Como en años anteriores, se incluye en la Memoria un apartado dedicado a la *"Agencia en cifras"* con información estadística que permite valorar de manera gráfica la actividad desarrollada por la Agencia en 2009. Asimismo, la Memoria de 2009 vuelve dirigir a los

«Los proyectos e iniciativas puestos en marcha por la institución en los últimos años han permitido la existencia de una mayor concienciación social respecto a la protección de datos de carácter personal»

poderes públicos un catálogo de *"Recomendaciones"* con el fin de que éstos promuevan y pongan en marcha iniciativas, en ámbitos que merecen atención específica, que fomenten la efectiva garantía del derecho fundamental a la protección de datos.

En cualquier caso, quienes requieran una información más específica y amplia, pueden acudir a la documentación recogida en la página Web de la Agencia, (www.agpd.es), recientemente renovada con el fin de incrementar su utilidad práctica.

A nuestro juicio, resultará evidente para el lector que, en el mundo actual, son muchos los interrogantes y retos que se suscitan en todos los ámbitos y espacios posibles, para las autoridades garantes de la protección de la privacidad y la protección de datos. Por ello, un año más espero que los datos aportados en la presente Memoria permitan a todos sus destinatarios valorar nuestra apuesta permanente de crecimiento y mejora, el esfuerzo y empeño de todo el personal al servicio de la Agencia Española de Protección de Datos para desarrollar satisfactoriamente las funciones que tiene encomendadas, y el cada vez más importante papel que desempeña esta institución en la sociedad actual.

Artemi Rallo Lombarte
Director de la Agencia Española de Protección de Datos.

«La Memoria 2009 incorpora la información más destacada y ofrece un análisis de los principales indicadores que permiten evaluar el nivel de implantación de la normativa de protección de datos»

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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

< ÍNDICE >

1. UNA SOCIEDAD MÁS INFORMADA Y CONSCIENTE DE SUS DERECHOS

A. UNA MAYOR CONCIENCIACIÓN SOCIAL ANTE LOS RIESGOS EN INTERNET

La protección efectiva de los ciudadanos en el uso de sus datos personales exige no sólo un mayor conocimiento de la normativa que les protege y un ejercicio efectivo de los derechos que les reconoce sino, también, que su nivel de concienciación se adapte a los nuevos riesgos que afectan a su privacidad.

Si la preocupación de los ciudadanos quedara reducida a tratamientos tradicionales de su información personal como la recepción de publicidad postal no solicitada o la inclusión en los denominados ficheros de morosidad, resultaría difícil afirmar, por muy conocedores y activos que fueran en el conocimiento de las normas y en el ejercicio de sus derechos, que disfrutan de una protección efectiva.

Una valoración realista de sus garantías hace imprescindible analizar qué conocen sobre los riesgos que plantea el desarrollo tecnológico y los nuevos servicios en Internet y cómo reaccionan ante ellos.

Los datos del año 2009 permiten apreciar un incremento de la concienciación ciudadana ante estos retos.

El barómetro del Centro de Investigaciones Sociológicas (CIS) de septiembre de 2009 refleja, en relación con la confianza de los ciudadanos en Internet, que los usuarios creen que es el lugar en que la seguridad y privacidad de sus datos es más deficiente, considerando un 56,6% que es baja o muy baja.

Aunque se reconoce que Internet facilita la obtención de información y la comunicación entre las personas, más del 70% considera que su uso favorece la intromisión en la vida privada, citándose, como servicios que generan mayor desconfianza, las redes sociales, los servicios de mensajería y los chats. En particular, la inclusión de fotografías o videos propios o de familiares o amigos en Internet ofrece para el 76,7% de los ciudadanos poca o ninguna seguridad.

Esta preocupación es mayor respecto de los menores, considerando más del 80% de los ciudadanos que los menores de edad deben tener controles en el acceso a Internet.

Los datos que se han destacado confirman la tendencia que se apuntaba en la encuesta del CIS de 2008, lo que permite considerar que la inquietud ciudadana sobre los riesgos en Internet no es meramente coyuntural, sino una realidad consolidada.

La AEPD ha realizado un esfuerzo específico para impulsar el conocimiento ciudadano de los riesgos en Internet y para poner a su disposición medidas adecuadas para evitarlos.

La Agencia ha realizado en colaboración con en el Instituto Nacional de Tecnologías de la Información (INTECO) un estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on-line que incluye un análisis jurídico, sociológico y tecnológico de estos servicios, así como recomendaciones y consejos dirigidos a fabricantes y proveedores de servicios de seguridad informática, prestadores de servicios de acceso a Internet, administraciones e instituciones públicas y, especialmente, a usuarios de las redes sociales.

Con una perspectiva más general, se actualizó la guía de las recomendaciones a usuarios de Internet que analiza los principales riesgos que aparecen actualmente en la Red y enumera recomendaciones para tratar de prevenir sus efectos. La guía destaca la necesidad de proteger a los menores en la red y apela a la responsabilidad de los internautas en el entorno de la llamada web 2.0, ante las posibilidades de difusión de información personal propia o de terceros que ofrecen servicios como las redes sociales o blogs.

Pero no cabe duda de que han sido los medios de comunicación los que han jugado un papel decisivo en la concienciación de los ciudadanos.

El año 2009 marca un antes y un después en la oferta de informaciones que permiten concienciar a los ciudadanos sobre los riesgos en Internet.

Si bien asuntos como la publicidad telefónica, la videovigilancia, algunas resoluciones y actuaciones destacadas de la AEPD, y la celebración en España de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, han ocupado gran parte de la actividad informativa de la AEPD durante el pasado año, lo cierto es que los medios de comunicación han centrado mayoritariamente su atención informativa en la incidencia de las nuevas tecnologías en la privacidad de los ciudadanos, y más concretamente en los riesgos asociados a servicios como las redes sociales. Ésta, sin duda, ha sido la principal temática abordada en numerosos y destacados reportajes y noticias aparecidas en distintos medios de comunicación, con una importante presencia en el medio audiovisual, así como en distintos proyectos de concienciación promovidos por medios de comunicación.

La AEPD ha reconocido esta sensibilidad de los medios de comunicación y su labor de difusión otorgando los Premios de comunicación y difusión de 2009 a espacios como "12 meses 12 causas" de la cadena Telecinco, la sección semanal sobre "Protección de datos en Radio 5 todo noticias" y a un proyecto documental para informar a los menores ante las nuevas tecnologías, que han destacado en el compromiso de concienciación ciudadana en Internet.

La labor de concienciación que están desarrollando los medios es aún más destacable si se tiene en cuenta que viene a suplir, desde el punto de vista de la información, las carencias del sistema educativo en estos ámbitos.

Reiteramos la felicitación a los medios de comunicación por impulsar que el objetivo de la AEPD "los ciudadanos, nuestra prioridad", alcance nuevas cotas para la protección del "ciudadano digital".

B. LOS CIUDADANOS MÁS SENSIBILIZADOS CON SUS DERECHOS

La mayor concienciación sobre el uso de Internet se complementa con un mayor conocimiento por los ciudadanos de los derechos que les asisten y una demanda creciente a la AEPD para garantizarlos.

El barómetro del CIS antes citado ofrece algunos indicadores significativos de esta tendencia:

- El porcentaje de ciudadanos preocupados por la protección de datos y el uso de la información personal continúa creciendo y alcanza al 74,1% de los encuestados.
- El conocimiento de una ley que proteja contra los posibles abusos que puedan producirse con su información personal se mantiene en torno al 50% de los ciudadanos.
- El conocimiento de la AEPD como entidad que garantiza sus derechos se incrementa superando por primera vez la barrera del 50% de la población.
- El porcentaje de ciudadanos que valoran de manera alta la seguridad de sus datos se mantiene entre el 50% y el 60% en los bancos, hospitales y Administraciones Públicas.
- La recepción de publicidad telefónica o a través de SMS, de una entidad a la que no se han facilitado los datos, crece levemente hasta alcanzar casi el 70% de los encuestados, mientras que la recepción de correos electrónicos no solicitados se eleva hasta el 83%.
- El porcentaje de ciudadanos que no da el consentimiento para el uso de los datos al rellenar un formulario que incluye una casilla al efecto se aproxima al 50%.

La demanda de información al Servicio de Atención al Ciudadano confirma la sensibilización sobre la protección de datos personales y permite perfilar las inquietudes más habituales.

El total de consultas planteadas a través de los canales telefónico, presencial y escrito se incrementó en un 33,82% aproximándose a la cifra de 100.000 consultas.

El mayor crecimiento se produce en el canal telefónico y, en menor medida en la atención por escrito, destacando que la mayor parte de estas consultas se contestaron a través del buzón electrónico de consultas ciudadano@agpd.es. Asimismo, los accesos a la página web alcanzaron la cifra de 3.000.000 con un incremento superior a 700.000 sobre el año anterior, lo que supone un promedio diario de 8.214,4 accesos.

Asimismo, se han incrementado en casi un millón el número de consultas al RGPD, aproximándose a la cifra de dos millones y medio de consultas.

El análisis de las consultas planteadas indica que la videovigilancia ha pasado a ocupar un lugar destacado en las inquietudes de los ciudadanos con preguntas como las siguientes:

- ¿Pueden el presidente y los miembros de la Junta de Gobierno exigir al administrador el visionado de las grabaciones?
- ¿Puede el inquilino de una finca instalar una cámara oculta que filme día y noche todo lo que ocurre en la entrada de la finca y en el jardín que es de uso privado de la propiedad y sus familiares o amigos?
- ¿Puede filmar a menores de edad en el jardín o en la piscina?
- ¿Qué nivel de seguridad tienen las imágenes obtenidas por cámaras de videovigilancia?

Junto a ellas se mantienen otras preocupaciones ya constatadas por la AEPD en relación con la publicidad y los ficheros de morosidad en consultas como:

- ¿Cómo puedo evitar que me sigan mandando publicidad no deseada?
- ¿Cómo desaparecer de las guías telefónicas o de los ficheros comerciales?
- ¿Cómo informarme si estoy en la lista de morosos?
- ¿Es legal incluir en un fichero de morosos sin notificar la inclusión?
- ¿Cómo darse de baja en estos ficheros?
- ¿Es legal que una tercera empresa reclame una deuda en nombre de otra?

Las solicitudes de información sobre el acceso a la historia clínica se ha consolidado como una de las preguntas frecuentes y empiezan a tener relevancia otras que indican nuevas inquietudes relacionadas con la tecnología, tales como:

- ¿Cómo hacer para desaparecer de una página web?
- ¿Es obligatorio inscribir los ficheros de geolocalización de los trabajadores?
- ¿El escaneado de bluetooth que reporta información sobre teléfonos móviles entra dentro de la LOPD?

De la encuesta de la AEPD para medir la satisfacción de los ciudadanos sobre este servicio en los canales presencial y telefónico, destacan los siguientes aspectos.

En el canal presencial:

- Los ciudadanos que han declarado tener conocimientos de la información que suministra la Agencia, antes de realizar la consulta se han incrementado llegando al 57,3%.
- El porcentaje que ha declarado que la información recibida fue satisfactorio o muy satisfactoria, creció hasta el 58,6%.
- Los encuestados que se declararon satisfechos o muy satisfechos sobre el tiempo de espera en ser atendidos y sobre la atención y servicio general se mantiene por encima del 91%.

En el canal telefónico, que es el más utilizado, se superan los altos índices de calidad de 2008, oscilando entre el 99,88% y el 100% las personas satisfechas con la información recibida, los conocimientos de quien les atendió y la corrección en el trato por el operador.

C. NUEVAS INQUIETUDES: ¿CÓMO DESAPAREZCO DE UNA PÁGINA WEB? ¿TENGO QUE RESIGNARME A ESTAR EXPUESTO EN INTERNET? ¿CÓMO EJERZO MI DERECHO AL OLVIDO?

El mayor conocimiento de la normativa de protección de datos se ha traducido en una conducta más activa en el uso de los instrumentos de autoprotección contemplados en ella, como son el ejercicio directo de sus derechos ante quienes tratan su información personal.

El ejercicio de derechos se ha incrementado cuantitativamente y, también, cualitativamente poniendo de manifiesto las nuevas inquietudes de los ciudadanos. El fuerte incremento de las reclamaciones ante la Agencia en solicitudes de tutelas de derecho se consolida e incrementa cerca de un 14% aproximándose a las 2.000 solicitudes.

Más significativo aún que este dato cuantitativo es el objeto de las reclamaciones planteadas que indican sus nuevas inquietudes. Las solicitudes de cancelación de los datos o de oposición al tratamiento de los mismos por los buscadores de Internet, aún no siendo muy numerosas en valores absolutos, se han incrementado en un 200%. Lo que revela que cada vez es mayor el interés mostrado por los ciudadanos para que no aparezcan sus datos personales en los índices que ofrecen los servicios de búsqueda en Internet a partir de los datos identificativos de una persona.

Los ciudadanos se preguntan ¿tengo que soportar estar expuesto en Internet? La respuesta es NO. De los casos planteados ante la AEPD, relacionados con la publicación de sus datos en ediciones digitales de diarios oficiales o medios de comunicación, destacan los siguientes:

- Publicación de sanciones administrativas ya cumplidas.
- Publicación por edictos de deudas vencidas.
- Sanciones disciplinarias a funcionarios de prisiones que afectan a su seguridad.
- Publicación de datos de una mujer y sus hijos menores, victimas de violencia doméstica que facilitan su localización para el cónyuge.
- Publicación en una página web que replica la edición electrónica de boletines oficiales de ayudas de exclusión social y desempleo.
- Publicación de indultos.

En esta materia, las resoluciones dictadas por la AEPD van en la línea de exigir que se adopten las medidas necesarias para evitar la indexación de los datos de carácter personal. También ha habido que tener en cuenta las posibles acciones que los webmasters pudiesen adoptar encaminadas a hacer efectivo el derecho solicitado por el particular. Esta nueva inquietud se confirma por el incremento de preguntas formuladas al Servicio de Atención al Ciudadanos sobre cómo hacer para desaparecer de una página web.

En 2009 destaca también el aumento de las reclamaciones relacionadas con la inclusión de los datos por motivos de morosidad en ficheros de información sobre solvencia patrimonial y crédito.

Al margen de estas cuestiones las principales preocupaciones de los ciudadanos siguen siendo: ¿Quién tiene mis datos?, ¿Cómo los cancelo?

Así resulta del importante incremento de las resoluciones relacionadas con la tutela de los derechos de acceso (Δ 59%) y de cancelación (Δ 40,8%) sumando sólo estas últimas un total de 1.366 resoluciones, cifra superior al total de las dictadas en el año anterior.

Conclusión que se confirma con las consultas al Servicio de Atención al Ciudadano sobre el ejercicio de derechos, en las que las relacionadas con los derechos de acceso y cancelación son el 20,62% y el 61,36%, respectivamente.

Es también novedoso el fuerte crecimiento de las resoluciones sobre el derecho de oposición (Δ 470%) que, en años anteriores, ocupaban el último lugar superando a las relacionadas con el derecho de rectificación.

En el caso de los derechos de acceso y oposición, la mayor parte de las resoluciones fueron estimatorias de los derechos de los ciudadanos, sucediendo lo contrario respecto de los derechos de cancelación y rectificación.

Para entender el elevado número de desestimaciones del derecho de cancelación, hay que tener en cuenta que, en muchos de los casos, se refieren a la cancelación de datos en los ficheros de solvencia patrimonial y de crédito en los que, al quedar confirmada la deuda por el acreedor, los responsables de dichos ficheros han actuado conforme a la normativa de protección de datos.

Asimismo, cuando se ha pedido la cancelación de datos a determinados organismos administrativos que se rigen por sus procedimientos específicos, se desestiman las solicitudes.

Las principales solicitudes de cancelación son las siguientes:

- Cancelación de anotaciones en informes técnicos realizados por profesionales en el ejercicio de sus funciones.
- Supresión de los datos una vez concluida la prestación de los servicios contratados; especialmente con operadores de telecomunicaciones.
- Supresión de antecedentes policiales, penales y penitenciarios de las administraciones públicas competentes.

- Cancelación de datos en foros de Internet.
- Datos en historiales clínicos.
- Supresión de datos o documentos que figuren en papel dentro de expedientes.

Respecto del derecho de acceso las cuestiones más relevantes son:

- Valoración de solvencia económica realizada por entidades financieras.
- Historial clínico de familiar fallecido.
- Historia clínica que se considera se ha suministrado de manera incompleta.

Sobre el derecho de rectificación destacan:

- Rectificar las bases de cotización contenida en ficheros de la Seguridad Social.
- Datos bancarios disponibles por otra empresa.

Y, en cuanto al derecho de oposición cabe reseñar los siguientes:

- Reflejar en los acuses de recibo el DNI del personal del Servicio de Correos y Telégrafos que realiza la entrega del correo.
- Recepción de publicidad de una empresa con la que se tiene contrato.

2. GARANTIZAR EL EFECTIVO Y EFICAZ CUMPLIMIENTO DE LA LOPD

A. FACILITAR EL CUMPLIMIENTO DE LA LEY: UNA GARANTÍA PARA LOS CIUDADANOS

El año 2008 supuso un punto de inflexión en política informativa de la Agencia dirigida a facilitar el cumplimiento de la normativa de protección de datos.

En 2009 la Agencia ha intensificado esta política informativa en la convicción de que facilitar el cumplimiento de la ley se traduce en un incremento de las garantías de los ciudadanos.

En el mes de enero se celebró la II Sesión Anual Abierta de la LOPD, con asistencia de alrededor de 700 participantes representativos de grandes corporaciones, consultores, Pymes, agentes sociales y Administraciones Públicas. En ella se informó y debatió sobre las principales novedades en la aplicación práctica del RLPOD y se dio respuesta a las inquietudes formuladas previamente por los participantes.

Asimismo, se ha ampliado el catálogo de guías prácticas para la difusión de la LOPD mediante la edición de las siguientes publicaciones:

- Guía de recomendaciones a usuarios de Internet.
- Guía de videovigilancia.
- Guía para la protección de datos en las relaciones laborales.

Además, se han editado las ediciones en inglés de la Guía de videovigilancia y de la Guía de Derechos de niños y niñas y deberes de los padres y madres.

El Servicio de Atención al Ciudadano continúa siendo un cauce de gran utilidad en la política informativa de la Agencia, como se desprende de los importantes crecimientos de las consultas atendidas año tras año.

Es, asimismo, un indicador de los temas prioritarios para los ciudadanos y los responsables del tratamiento de datos personales. Las preguntas más frecuentes que se han planteado se refirieron a las siguientes cuestiones:

- Obligaciones de una empresa que tiene ficheros con datos personales.
- ¿Cómo se debe inscribir un fichero?
- Formularios de inscripción y cómo obtenerlos.
- Si se incluyen o no los empresarios individuales y las personas de contacto de la empresa.
- Tratamientos de datos de empresas que operan en Sudamérica.
- Acceso a los historiales clínicos.
- Amparo de derechos de personas fallecidas.
- Si el cartel informativo de la videovigilancia puede colocarse en lenguas cooficiales distintas del castellano.
- Aplicación de la Ley 25/2007, de conservación de datos, respecto del alta de servicios de usuarios en general y de menores de edad en particular.
- Si es obligatorio inscribir los ficheros de geolocalización de trabajadores.
- Si el escaneado de Bluetooth que reporta información sobre teléfonos móviles entra dentro de la LOPD.
- Si es necesario inscribir un fichero sobre clientes afectados por blanqueo de capitales que son de dominio público.

En lo que se refiere a consultas de mayor complejidad, en 2009 se atendieron por el Gabinete Jurídico 679 consultas (cifra prácticamente idéntica a la de 2008, de las cuales 359 (54%) fueron planteadas por las Administraciones Públicas y 313 (46%) por el sector privado.

Se mantiene así el incremento producido respecto de volumen de consultas de 2008, cuyas causas probablemente se encuentren relacionados con la entrada en vigor del Reglamento de la Ley Orgánica 15/1999, al que se dedican buena parte de las cuestiones. En cuanto al reparto de las consultas de los sectores público y privado, y frente a la modificación producida en 2008, en que aumentaron considerablemente las consultas referidas al sector privado, se ha retomado la pauta habitual de similitud en el número de las mismas, si bien en este ejercicio se observa un notable incremento del peso del sector público (del 40% en 2008 al 54% en 2009).

En cuanto a las materias objeto de consulta, debe hacerse referencia a las siguientes:

- Cesiones de datos.
- Protección de datos en el sector de las comunicaciones electrónicas.
- Concurrencia de causas legitimadoras del tratamiento, con especial referencia a los requisitos exigibles para la adecuada obtención del consentimiento.
- Especialidades referidas al tratamiento y cesión de datos en ficheros de titularidad pública y la delimitación de dichos ficheros frente a los de titularidad privada.
- Aplicación del Reglamento de desarrollo de la LOPD, en particular en relación con las medidas de seguridad.
- Videovigilancia.
- Delimitación del ámbito de aplicación objetivo y territorial de las normas de protección de datos.
- Régimen del encargado del tratamiento.

En particular, de esta distribución sectorial se desprenden las siguientes conclusiones:

- El especial incremento (142%) de las consultas relacionadas con la delimitación de los conceptos de ficheros de titularidad pública y privada y los requisitos exigibles a estos últimos.
- Igualmente es importante el incremento de las cuestiones relacionadas con el sector de las comunicaciones electrónicas y la aplicación al mismo de la LOPD y su normativa sectorial (91%).
- La relevancia mayor en este ejercicio de las consultas relacionadas con el cumplimiento de los principios de calidad de datos y, en particular, de los informes que se centran en el análisis del cumplimiento del principio de proporcionalidad.
- El mantenimiento de un número relevante, que incluso se incrementa ligeramente, de las consultas relacionadas con la videovigilancia.
- La disminución cuantitativa de cuestiones que resultaron especialmente reiteradas en el año 2008, pese a mantener un importante volumen en términos comparativos con las restantes. Así sucede en relación con las consultas relativas al ámbito de aplicación de la legislación de protección de datos, el cumplimiento del deber de información, el tratamiento de datos especialmente protegidos o la normativa de seguridad contenida en el Reglamento de desarrollo de la LOPD.

Atendiendo a la distribución sectorial de las consultas del sector privado, debe hacerse referencia a los siguientes sectores principales:

- Telecomunicaciones y sociedad de la información.
- Particulares.
- Asesoría y consultoría.
- Asociaciones empresariales y profesionales.
- Sanidad y farmacéuticos.
- Distribución y venta.

- Servicios informáticos.
- Educación y enseñanza.
- Banca y seguros.

De dicha distribución deben extraerse las siguientes conclusiones relevantes:

- El descenso en más de un 65% de las consultas procedentes de entidades dedicadas a la asesoría y consultoría, dado que transcurrido más de un año desde la entrada en vigor del Reglamento. La Agencia ha vuelto a mantener el criterio general de atender únicamente las consultas relacionadas con sus ficheros y tratamiento y no con las de sus clientes, que deberán formularse por éstos últimos.
- La relevancia adquirida en este ejercicio por las consultas procedentes de particulares y de empresas vinculadas con el ámbito sanitario y el sector de las telecomunicaciones.
- El mantenimiento de la importancia de las consultas procedentes de asociaciones empresariales y profesionales y del sector del transporte.
- La disminución del volumen de consultas procedentes del bancario y del de la publicidad y prospección comercial.

En cuanto a las cuestiones concretas que han sido analizadas y sus conclusiones, se han reiterado las que figuran en la Memoria de 2008 a las que se añaden como novedad las siguientes:

- Interpretación del alcance que habrá de darse a las exclusiones a la normativa de protección de datos contenidas en los apartados 2 y 3 del artículo 2 del Reglamento (datos de contacto y empresarios individuales).
- Los informes preceptivos emitidos a instancia de la Comisión del Mercado de las Telecomunicaciones en los procedimientos de autorización de acceso a los directorios de abonados para la prestación de servicios de guías consulta telefónica o servicios de emergencia.
- La emisión de informes jurídicos a requerimiento del Defensor del Pueblo en relación con materias tales como el tratamiento por los Colegios de Procuradores de datos relacionados con los asuntos en que ha participado un colegiado; la naturaleza de las empresas de recobro a los efectos de la aplicación de las normas de protección de datos; determinadas cuestiones relacionadas con los ficheros de solvencia patrimonial y crédito o los derechos de los abonados en relación con los directorios de comunicaciones electrónicas.
- Los relativos a la implantación y desarrollo del Sistema de Información del Sistema Nacional de Salud y de la Historia Clínica Única en todo el Sistema Público de Salud.
- Las relativas a los tratamientos llevados a cabo por los servicios de prevención en el marco de la Ley de Prevención de Riesgos Laborales, el acceso a datos de salud por el empresario y el tratamiento y comunicación de datos por las mutuas de accidentes de trabajo.
- La resolución de cuestiones concretas relacionadas con los ficheros mantenidos por los sujetos obligados en el marco de las exigencias contenidas en la legislación de blanqueo de capitales y de la financiación del terrorismo.
- Las relacionadas con la posible publicidad a través de Internet de diversos registros administrativos, tales como los gestionados por la Dirección General de Seguros y Fondos de Pensiones.
- La licitud de la comunicación por las líneas aéreas a las autoridades del Reino Unido de determinados datos de los pasajeros con carácter previo a la salida del vuelo con base en la legislación de inmigración del Reino Unido.
- La resolución de determinadas cuestiones relacionadas con la legalidad de la asunción por la empresa absorbente de las obligaciones de la entidad absorbida en procesos de fusión y la posibilidad de que los datos sean migrados durante el proceso de fusión.
- Las especialidades del tratamiento de datos relacionados con los menores, atendiendo a determinados entornos concretos (por ejemplo, redes sociales) y la exigibilidad de medidas de comprobación de la edad del menor.
- La garantía del cumplimiento del deber de informar en casos especiales como la contratación telefónica.

- La delimitación del ámbito de aplicación territorial de la Ley Orgánica de Protección de Datos en el supuesto de sucursales de empresas extracomunitarias o de encargados del tratamiento ubicados en territorio español.

- La comunicación de los datos contenidos en los documentos TC2 del subcontratista al contratista principal durante el período de ejecución de la subcontrata.

- La improcedencia de que se comuniquen a las centrales sindicales los datos referidos a la productividad o gratificaciones extraordinarias del personal funcionario.

- La viabilidad del acceso por empresas municipales a los datos del padrón municipal para la gestión de servicios públicos y, en particular, la delimitación de los supuestos en que las mismas son responsable o encargadas del tratamiento.

- Los requisitos legalmente exigibles para la creación de los denominados "ficheros de exclusión" publicitaria o "listas Robinson" y, en particular del creado a tal efecto por la Federación Española de Comercio Electrónico y Marketing Directo.

- Los requisitos legalmente exigibles para la puesta en funcionamiento por parte de diversas asociaciones de ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias y, en particular, la posibilidad de creación de los denominados "ficheros positivos", que contengan toda la información crediticia del afectado y no sólo la relativa a los incumplimientos de sus obligaciones, exigiendo la Ley española el consentimiento del afectado.

El Reglamento de desarrollo de la LOPD estableció un nuevo marco sobre la autorregulación promoviendo que los Códigos Tipo aporten valor añadido a la protección de datos personales y garanticen su aplicación efectiva.

Al término del plazo establecido para la adaptación de los Códigos Tipo inscritos en el RGPD al nuevo Reglamento, tres han sido cancelados por no responder a las nuevas exigencias y los restantes se han modificado para cumplirlas. No obstante, en el caso de los Códigos de odontólogos y estomatólogos de España y del sector de la intermediación inmobiliaria se advirtió expresamente que sus promotores deberán informar anualmente sobre el número de adheridos para evaluar la representatividad del sector.

Como principal novedad se ha inscrito el Código Tipo correspondiente al "Sistema de Autorregulación en materia de protección de datos: Investigación Clínica y Farmacovigilancia", promovido por FARMAINDUSTRIA.

El Código adapta las previsiones de la LOPD a actividades complejas como son los ensayos clínicos con medicamentos y la farmacovigilancia delimitando los ficheros correspondientes a tales actividades, aclarando la posición jurídica del amplio abanico de sujetos intervinientes y estableciendo procedimientos específicos para la disociación de los datos personales.

De este modo el Código constituye un referente básico para facilitar el cumplimiento de la normativa de protección de datos.

También se ha inscrito el Código Tipo para las entidades locales adheridas a la Asociación de Municipios Vascos. El código, tramitado por la Agencia Vasca de Protección de Datos, presenta como novedad el ser una primicia en la autorregulación por parte de las Administraciones Públicas.

Las políticas de divulgación y comunicación pública impulsadas por la Agencia continúan dando frutos.

En 2009 se han inscrito en el Registro General de Protección de Datos casi 400.000 nuevos ficheros, lo que supone un incremento superior al 50% respecto a 2008, alcanzando una cifra total de 1.647.756.

A este incremento ha contribuido el sistema simplificado de notificación de ficheros NOTA. Entre las facilidades que ofrece el sistema NOTA para la inscripción de ficheros destaca la notificación a través de Internet que se utiliza en cerca del 90% de los casos frente al 10% de las notificaciones manuales.

Además, se ha duplicado la presentación de notificaciones firmadas con certificado electrónico de firma que han llegado a las 100.000, lo que supone que una de cada cinco utiliza este formato.

A lo que se añade que otra de las opciones del sistema NOTA, como es la notificación mediante aplicativos desarrollados por terceros,

normalmente para realizar inscripciones masivas, han llegado a ser otro 20% del total de notificaciones. En definitiva, la oferta de nuevas tecnologías y la flexibilidad de las opciones para los responsables son el instrumento más eficaz para cumplir la Ley.

El incremento de las inscripciones es más fuerte en el ámbito privado que ha crecido en un 63%, principalmente en el entorno de las pequeñas y medianas empresas en los sectores de comercio, sanidad, contabilidad, auditoria y asesoría fiscal, construcción, turismo y hostelería.

En el sector público destaca un incremento cercano al 50% en los ficheros de la Administración Local con lo que los ficheros de Ayuntamientos inscritos en el RGPD, representan casi el 96% de la población española.

Atendiendo a la sensibilidad de los datos incorporados a los ficheros son reseñables los incrementos tanto de los que declaran datos de ideología, creencias, religión y, sobre todo, afiliación sindical, como de los que declaran datos de salud, origen racial y vida sexual. Al finalizar 2009 los primeros ascienden a más de 53.000 en el ámbito privado y a más de 17.000 en el público. Los segundos alcanzan cifras en torno a 238.000 y 26.000 en uno y otro ámbito, respectivamente.

En cuanto a las finalidades de los ficheros privados es significativo el crecimiento, superior al 30%, de los que tienen por objeto el análisis de perfiles de las personas, habitualmente relacionados con el sector de la publicidad. Lo que es un indicador del desarrollo de fórmulas publicitarias cada vez más intrusivas en la privacidad.

La oferta de nuevas herramientas para facilitar el cumplimiento de la Ley ha dado un salto cualitativo con el programa EVALUA presentado en el marco de la 31ª Conferencia Internacional de Protección de Datos y de la Privacidad.

EVALUA es una herramienta gratuita on-line para autoevaluar el cumplimiento de la LOPD para las empresas y las Administraciones Públicas.

Para ello ofrece respuestas a las dudas a las que se enfrentan habitualmente quienes tratan datos personales mediante un autotest basado en preguntas con respuesta múltiple.

El programa contempla dos niveles de autoevaluación con dos perfiles distintos de usuario. El primero es un test básico para quienes toman un primer contacto con la LOPD que les permite conocer el nivel de cumplimiento de la normativa. El segundo, para usuarios con un mayor nivel de conocimiento, permite verificar fácilmente el cumplimiento de las medidas de seguridad.

EVALUA utiliza un lenguaje claro y ofrece documentación de apoyo y ayuda para facilitar la comprensión de las preguntas. Su uso garantiza el anonimato del usuario, es gratuito y una vez terminado genera un informe con recomendaciones personalizadas.

B. UN AFÁN PERMANENTE POR LA SEGURIDAD JURÍDICA

Garantizar la sistemática de ordenamiento jurídico con la normativa de protección de datos supone avanzar en la consecución de mayores niveles de seguridad jurídica.

La AEPD ha continuado trabajando en el objetivo de lograr mayor seguridad jurídica a través de los informes preceptivos sobre disposiciones de carácter general.

De este modo fueron informadas 100 disposiciones, entre las que cabe hacer referencia a las siguientes:

- Las adoptadas en desarrollo de la Ley 11/2007, de Acceso electrónico de los ciudadanos a los Servicios públicos (Proyecto de Real Decreto de desarrollo parcial, Proyectos de Reales Decretos por los que se aprueban el esquema nacional de interoperabilidad y el esquema nacional de seguridad y Proyecto de Orden por la que se crea el registro Electrónico Común de la Administración General del Estado).

- En materia económica, ha sido informado en dos ocasiones el Anteproyecto de Ley de Prevención del Blanqueo de Capitales y la financiación del terrorismo.

- En el ámbito sanitario, el Proyecto de Real Decreto por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, el Proyecto de Real decreto por el que se modifica el Reglamento General de Mutualismo Adminis-

trativo y el Proyecto de Real Decreto de regulación de la receta médica y la orden hospitalaria de dispensación.

- El Proyecto de creación de la Historia clínica electrónica única en el ámbito de MUFACE, a través del informe emitido al Proyecto de Orden de creación del correspondiente fichero.

- El Anteproyecto de Ley Orgánica de salud sexual y reproductiva y de la interrupción voluntaria del embarazo.

- El Anteproyecto de Ley sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea.

- El Proyecto de Real Decreto por el que se aprueba el Reglamento de los Archivos Judiciales Militares.

- Los Acuerdos entre la Unión Europea y Australia y entre la Unión Europea y Estados Unidos sobre el tratamiento y transferencia de datos generados en la Unión Europea del Registro de nombres de pasajeros (PNR).

- Por último, fueron informadas diversas disposiciones de creación de ficheros de los Ministerios de Economía y Hacienda, Industria, Turismo y Comercio, Fomento, Trabajo e Inmigración, Defensa, Medio Ambiente, Medio rural y Marino, Justicia, Sanidad y Política Social, Asuntos Exteriores y Cooperación, Interior, Cultura y Ciencia e Innovación, así como de los del Tribunal de Cuentas y de la Casa de S.M. el Rey.

Por otra parte, el análisis del grado de seguridad jurídica en la aplicación de la LOPD obliga a contemplar en qué medida las Resoluciones de la AEPD son ratificadas o revocadas por los Tribunales.

Antes de proceder al análisis concreto de la doctrina judicial emanada del Tribunal Supremo y de la Audiencia Nacional, es preciso poner de manifiesto el singular efecto que sobre las cifras relativas al total de sentencias dictadas por ambos órganos, y en particular por el Tribunal Supremo, ocasionan los recursos relacionados con el ejercicio del derecho de cancelación de los datos existentes en los Libros de Bautismo de la Iglesia Católica.

En total, en relación con esta materia durante el año 2009 se han dictado 99 sentencias en primera instancia por la Audiencia Nacional (un 29% del total) y el Tribunal Supremo ha resuelto 163 recursos de casación (más del 90% del total) en el sentido sostenido en su sentencia de 19 de septiembre de 2008, de cuyo contenido y consecuencias se dio sobrada cuenta en la Memoria correspondiente a dicho ejercicio.

Teniendo en cuenta esta circunstancia, el análisis que se realizará a continuación no tendrá en cuenta el volumen de sentencias relacionadas con la cancelación de los datos de los libros de bautismos, a fin de poder ofrecer una información significativa.

Así durante el año 2009 se han dictado, respectivamente, por la Sala de lo contencioso-administrativo de la Audiencia Nacional y por la del Tribunal Supremo 240 y 8 Sentencias.

En cuanto a las Sentencias de la Audiencia Nacional:

- 162 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (68%).

- 17 estimaron parcialmente los recursos (7%).

- 61 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (25%).

En relación con los sectores de actividad a los que afectan las sentencias dictadas se mantiene en parte la tendencia sostenida en ejercicios anteriores. No obstante, son más que significativos los incrementos producidos en los sectores financiero, banca y seguros (un 138%), en el sector de agua y energía (un 178%) y de distribución (un 100%).

También se han incrementado muy significativamente los recursos interpuestos por particulares contra resoluciones de archivo dictadas por la Agencia, que ya constituyen casi un 10% de los recursos resueltos, siendo también significativo el incremento de un 70% en las sentencias en que los recurrentes son sindicatos y asociaciones.

Al propio tiempo, se mantiene la relevancia de las sentencias relacionadas con las Administraciones Públicas y disminuyen aquéllas en que los recurrentes son entidades gestoras de ficheros de solvencia patrimonial y crédito.

En cuanto a las materias, siguen siendo especialmente significativas las referidas a la inclusión de datos inexactos en ficheros de solvencia patrimonial y crédito o con la contratación de servicios, en las que, junto con las pertenecientes al sector de las comunicaciones electrónicas, adquieren relevancia las empresas del sector energético.

También es preciso indicar que en un buen número de sentencias estimatorias, la decisión final del recurso se ha fundado en la ampliación de la prueba practicada por el Tribunal respecto a la realizada por la Agencia. En este sentido, conviene precisar que la mayor parte de los criterios estimatorios de la Audiencia Nacional se han fundado en una distinta interpretación de la prueba obrante en autos y no en discrepancias con las resoluciones recurridas en lo que a la aplicación de las normas sustantivas de protección de datos se refiere.

De las sentencias de la Audiencia Nacional cabe desatacar las siguientes:

- La SAN de 9 de enero de 2009 se refiere a un supuesto de aplicación de la LSSI, considerando que a los efectos de la aplicación de dicha Ley resulta enteramente irrelevante que las direcciones de correo electrónico a las que se realizaron las comunicaciones comerciales se encontrasen en fuentes accesibles al público, dado el carácter restrictivo del artículo 21 de dicha Ley. Al propio tiempo, considera que no puede considerarse masivo el envío de 45 correos electrónicos a distintos destinatarios en el plazo de un mes.

- Las SSAN de 14 de enero y 12 de noviembre se refieren a un supuesto de posible contratación fraudulenta por un menor en el ámbito de las telecomunicaciones, considerando las sentencias que, aún no constando el consentimiento del menor, cabe apreciar la existencia de dicho contrato en virtud de determinados indicios, tales como el abono del servicio y la realización de llamadas por y al menor por parte de sus familiares a la línea contratada.

- La SAN de 28 de enero de 2009 considera que no es materia propia de protección de datos la rectificación solicitada por un interesado de la información contenida en un expediente tramitado ante un Tribunal Económico-Administrativo regional.

- Las SSAN de 4 de febrero y 1 de octubre de 2008 consideran, siguiendo el criterio mantenido en otras sentencias citadas en la Memoria de 2008, que cuando un *listbroker* actúa en nombre propio ha de ser considerado responsable del fichero.

- Las SSAN de 13 de marzo, 22 de abril y 5 de mayo de 2009 resuelven los recursos tramitados en relación con el tratamiento de datos de personas públicamente relevantes llevado a cabo por un medio de comunicación social, desestimando las pretensiones de dichas personas.

- La SAN de 17 de marzo de 2009 resulta relevante por ser la única dictada hasta la fecha referida a un recurso interpuesto contra una autorización de transferencia internacional de datos. La sentencia desestima la pretensión de una organización sindical contra dicha autorización.

- Las SSAN de 25 de marzo, 4 de abril y 13 de julio de 2009 se refieren al supuesto en que una determinada entidad obtuvo, con la colaboración de otras dedicadas a la seguridad privada, datos relativos a la identificación, domicilio y otras informaciones relacionadas con los denunciantes que posteriormente fueron facilitadas a empresas de recobro. En estos supuestos, la entidad recurrente (la misma en los tres casos) alegaba que se había informado a los interesados acerca de este tratamiento sin que por aquéllos se hubiera hecho manifestación alguna en contrario, pero no se acreditaba en ninguno de ellos la recepción por el interesado de la citada información, por lo que la entidad fue sancionada por tratamiento ilícito de los datos y por su cesión a la empresa de recobro.

- La SAN de 16 de abril de 2009 considera que la sanción impuesta por la AEPD a un determinado partido político por el uso ilícito de los datos de personas no afiliadas al mismo para su inclusión en listas electorales no puede ser objeto de sanción por poder subsumirse en el correspondiente tipo penal aplicable a la misma conducta.

- La SAN de 22 de abril de 2009 considera que la grabación de la imagen de una determinada persona en un fichero de vídeo contenido en un CD aportado a un procedimiento judicial no está protegida por la LOPD, dado que dichos datos no estaban destinados a incorporarse a un fichero ni constituyen en sí mismos un fichero.

- La SAN de 29 de abril de 2009 consideró que no cabía apreciar la existencia de un tratamiento fraudulento de datos de carácter personal en un supuesto en que, habiéndose interpuesto querella criminal por el afectado por falsificación de su firma, las diligencias penales habían sido sobreseídas. Al propio tiempo, la sentencia señala que existen indicios contrarios a considerar tal carácter fraudulento como consecuencia de otras conductas desarrolladas por el interesado. En términos parcialmente similares pueden tenerse en cuenta las SSAN de 11 y 26 de junio y 29 de octubre de 2009.

- La SAN de 6 de mayo de 2009 se refiere igualmente a un supuesto de fraude en la contratación en el que si bien la Sala reconoce su existencia considera que no procede la imposición de la sanción a quien resultaba ser la prestadora del servicio sino al distribuidor que simuló el contrato y contra el que no se dirigió el procedimiento.

- La SAN de 24 de mayo de 2009 considera lícito el tratamiento llevado a cabo por una empresa de recobro que actualizó los datos referidos al domicilio y número de teléfono de un cliente de la entidad que había suscrito con la misma un contrato de encargado del tratamiento, al considerar que el tratamiento de tales datos y su actualización no requieren el consentimiento del afectado al encontrarse amparados en la relación contractual existente entre el afectado y la entidad acreedora.

- La SAN de 11 de junio de 2009 está referida a la posible vulneración del deber de secreto como consecuencia de la inclusión de datos en un foro de Internet. La sentencia considera que la infracción debe entenderse cometida en el momento en que la información es incluida en el foro, dado que quien la incluyó, al no ser administrador del mismo, no podía suprimirla con posterioridad.

- La SAN de 11 de junio de 2009 considera vulnerado el deber de secreto por una entidad local, por cuanto habiéndose solicitado de la misma por el interesado la emisión de una certificación relativa a los servicios prestados en el mismo para su aportación en un proceso selectivo de otra administración, se facilitó por la entidad local dicha información a esa segunda administración.

- La SAN de 18 de junio de 2009 confirma los criterios que en materia de videovigilancia fijó la AEPD en la Instrucción 1/2006 y aclara que la grabación a través de videocámaras de la vía pública por parte de una determinada empresa resulta contraria al principio de proporcionalidad previsto en el artículo 4.1 de la LOPD.

- La SAN de 18 de junio de 2009 se refiere a un supuesto en que fueron encontrados documentos con datos personales en la vía pública y considera que no se produjo vulneración del deber de secreto, dado que la información no fue conocida por terceros, pero que procede la imposición de la sanción por vulneración del deber de seguridad por cuanto sí se había producido un incumplimiento de las medidas exigibles.

- La SAN de 9 de julio considera que la emisión de una carta de despido por un empresario en la que se incluyen datos de salud del afectado no está sometida a la LOPD, dado que no consta que la misma forme parte de ningún fichero de la empresa, conforme a la doctrina emanada de la STS de 19 de septiembre de 2008.

- La SAN de 9 de julio de 2009 considera desproporcionada la publicación en un medio de comunicación de imágenes referidas a una víctima de un atentado terrorista con lesiones cerebrales irreversibles, al entender que el carácter noticiable de la información se cumplía suficientemente sin la inclusión de tales imágenes, por lo que no cabe dar prevalencia a la libertad de información consagrada por el artículo 20 de la Constitución.

- La SAN de 24 de septiembre de 2009 considera que no procede imputar a una Administración Local la vulneración del deber de secreto ocasionada como consecuencia de la divulgación de ciertas informaciones llevada a cabo por parte de un miembro de la misma, a la que accedió en virtud de su cargo.

- La SAN de 9 de octubre de 2009 considera que los ficheros de los que es responsable el Ministerio Fiscal se encuentran sometidos a la LOPD y a las competencias supervisoras de la AEPD, considerando en el supuesto planteado que no procede la cancelación de determinados datos de un menor mantenidos en un fichero de la Fiscalía de Menores, al existir legitimación suficiente para su conservación.

- La SAN de 22 de octubre de 2009 considera que no puede apreciarse la existencia de una vulneración del deber de secreto y de la obligación de implantar las adecuadas medidas de seguridad cuando existe una conducta activa de los propios denunciantes tendente a violentar las medidas implantadas por el responsable del fichero.

- La SAN de 29 de octubre de 2009 considera que existe falta de culpabilidad en la infracción cometida por una federación deportiva, consistente en la publicación en un sitio web de las sanciones adoptadas en materia de dopaje, considerando que existe en la misma confianza legítima al haber seguido las directrices establecidas por el Consejo Superior de Deportes.

- La SAN de 19 de noviembre de 2009 considera, conforme al criterio mantenido por la Agencia, que el acceso por el personal de Juzgados y Tribunales a la base de datos de determinados funcionarios de la AEAT en virtud del Acuerdo de colaboración entre el CGPJ y la citada Agencia está amparado por la relación estatutaria de los funcionarios con la Administración, siendo necesarios para el ejercicio de funciones propias de las Administraciones Públicas y en el ámbito de sus competencias.

- La SAN de 26 de noviembre de 2009 confirma las sanciones impuestas por la Agencia en un supuesto en que una entidad recogió datos de un menor de edad sin contar con el consentimiento de sus padres o tutores, utilizándolos posteriormente para la realización de una campaña mediante la que se ofreció al mismo una tarjeta de crédito.

- La SAN de 19 de diciembre de 2009 considera que debe apreciarse la existencia de un concurso medial entre las infracciones de los artículos 4.3 y 6.1 de la LOPD, dado que si los datos han sido tratados sin consentimiento del interesado no cabe entender que es sancionable el que los mismos sean inexactos.

- Por otra parte, son numerosas las sentencias en que, frente a la alegación de la recurrente acerca de la existencia de un uso fraudulento o abusivo por parte de la AEPD del trámite de diligencias previas, la Audiencia Nacional ha puesto de manifiesto la improcedencia de dicha alegación atendiendo al incremento de la carga de trabajo producida en la Agencia, siguiendo el criterio ya establecido en la SAN de 19 de noviembre de 2008.

Por su parte, el Tribunal Supremo, y también sin hacer referencia a las sentencias referidas a los Libros de Bautismo de la Iglesia Católica, dictó las siguientes resoluciones:

- Declaró en trece sentencias no haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así confirmadas.

- Declaró en dos supuestos haber lugar al recurso interpuesto por la representación procesal de la Agencia contra sentencias que estimaban recursos interpuestos contra sus resoluciones. En uno de los casos, la sentencia de instancia estimaba el recurso contra una resolución en que se imponían dos sanciones (una grave y otra muy grave), siendo sólo la segunda de ellas susceptible de recurso.

- Declaró en un supuesto haber lugar al recurso interpuesto por un responsable contra la sentencia de la Audiencia Nacional que estimaba, a su vez, el recurso interpuesto por los afectados contra una resolución de archivo de actuaciones dictada por la Agencia, que fue confirmada así por el Tribunal Supremo.

- Declaró en tres supuestos no haber lugar al recurso interpuesto por la representación procesal de la Agencia (que en este caso coincidía con la de la responsable del fichero, al ser ésta la Agencia Estatal de la Administración Tributaria, defendidas ambas por el Abogado del Estado) contra una sentencia que estimaba el recurso interpuesto contra la resolución de esta Agencia.

En consecuencia, y al margen de las cuestiones ya señaladas, el Alto Tribunal vino a ratificar los criterios de la Agencia en 16 de las 19 ocasiones en que la cuestión fue sometida a su parecer.

Dicho lo anterior, debe hacerse referencia a las siguientes sentencias:

- Las SSTS de 14 de enero y 17 de julio de 2009, declara no ha lugar el recurso de casación para la unificación de doctrina, dado que no concurren las circunstancias exigidas por la ley de la jurisdicción como necesarias para poder apreciar la contradicción entre sentencias de identidad sustancial.

- La STS de 27 de enero de 2009 declara no haber lugar al recurso de casación referente a la cesión de datos entre dos empresas de un mismo grupo empresarial, sin el consentimiento inequívoco de los clientes. En el mismo sentido se pronuncia la STS de 28 de abril de 2009.

- La STS de 24 de febrero de 2009, declara no haber lugar el recurso de casación, refiriéndose a la adecuada inclusión de determinados datos en ficheros de solvencia patrimonial y crédito, confirmándose la SAN, que a su vez consideraba ajustada a derecho la resolución de la Agencia.

- La STS de 28 de abril de 2009 considera que se encuentra sometido a la LOPD el tratamiento de datos efectuado por una empresa para la realización de una campaña dirigida por una empresa ubicada en España a ciudadanos españoles aún cuando los datos se recogían en un servidor ubicado en Estados Unidos.

- La STS de 12 de mayo de 2009 declara haber lugar al recurso de casación interpuesto por el Abogado del Estado. Confirma la existencia de una cesión en un supuesto de tratamiento de datos que una entidad efectúa con respecto a otra, con la posterior remisión de un fichero enriquecido con los datos tratados.

- La STS de 3 de junio de 2009, declara no haber lugar al recurso de casación considerando que existe una vulneración de la LOPD como consecuencia de la cesión de datos de unos clientes sin su consentimiento a otra entidad, siendo irrelevante que exista entre ambas entidades un contrato, en el que los clientes nada tienen que ver.

- La STS de 7 de julio de 2009, declara no haber lugar al recurso de casación interpuesto por el Abogado del Estado. Reconociendo que la cesión de los datos, aunque lo ampara una ley, debe venir condicionada al cumplimiento de fines legalmente previstos, pudiendo el afectado tener conocimiento de quiénes son los destinatarios de las cesiones efectuadas mediante el ejercicio del derecho de acceso del art. 15 LOPD.

- La STS de 6 de octubre de 2009, considera inadmisible el recurso contencioso-administrativo interpuesto contra una resolución de archivo de actuaciones por falta de legitimación activa, destacando que el denunciante de una infracción de la legislación de

protección de datos carece de legitimación activa para impugnar la resolución de la agencia en lo que concierne al resultado sancionador del mismo.

- La STS de 20 de octubre de 2009, declarando haber lugar al recurso interpuesto por el Abogado del Estado, viene a confirmar la resolución por la que la Agencia sancionó a un servicio de prevención de riesgos laborales por utilizar los datos obtenidos del afectado cuando prestaba sus servicios en una empresa cliente del mismo para la valoración de la aptitud de ese trabajador cuando pasó a prestar servicios en otra empresa que tenía contratado el mismo servicio de prevención.

- Las STS de 23 de octubre y 17 de noviembre de 2009 confirman los criterios de la Agencia en relación con los supuestos de aparición de datos personales en la vía pública, en el sentido de considerar vulnerado el artículo 10 de la LOPD. En particular, la primera de ellas considera que el hecho de no haberse formulado denuncia por los afectados no puede ser tenido en cuenta a la hora de aplicar los criterios establecidos en el artículo 45.5 de la LOPD.

- La STS de 17 de noviembre de 2009 se refiere al alcance de la excepción al consentimiento para la cesión de datos a órganos judiciales, considerando que la misma sólo es aplicable en los supuestos en los que los datos son directamente solicitados por aquéllos.

- La STS de 2 de diciembre de 2009, declara no haber lugar al recurso de casación confirmando la SAN que a su vez consideraba ajustado a derecho el archivo de las actuaciones acordado por la Agencia, referido al tratamiento del dato de afiliación sindical, dado que la solicitud de descuento de cuota sindical fue interesada voluntariamente por los propios trabajadores afectados.

- Asimismo, diversas SSTS, como las de 29 de abril, 4 de mayo, 16 de septiembre, 14 de octubre y 17 de noviembre de 2009 se refieren a los requisitos exigibles para la verdadera existencia de un encargado del tratamiento, haciendo todas ellas hincapié en la necesidad de que exista un contrato escrito, cuya veracidad podrá examinarse por la Agencia Española de Protección de Datos y en que el encargado se limite a tratar los datos por cuenta del responsable y no en beneficio propio.

- En especial, la STS de 9 de octubre de 2009 se refiere al supuesto en que dos empresas contratan la prestación de un servicio a los clientes de la primera de ellas (la emisión de una tarjeta de pago de combustible) que implica para la segunda la obtención de un beneficio directo como consecuencia del uso de dicho servicio por los citados clientes, entendiendo que no existe duda de que nos encontramos ante una cesión de datos.

C. UNA DEMANDA CRECIENTE DE GARANTÍAS: UNA RESPUESTA ACTIVA DE LA AGENCIA

El crecimiento de la demanda ciudadana sobre sus derechos en materia de protección de los datos personales es un fenómeno incontestable.

En 2009 el número de reclamaciones planteadas ante la AEPD ha dado lugar a un incremento del 75% de las actuaciones iniciadas, que han llegado a superar las 4.100. A las que se añaden las relativas a la tutela de derechos citadas anteriormente.

Los principales sectores objeto de investigación han sido los de telecomunicaciones, entidades financieras y videovigilancia cuya incidencia en el total de actuaciones realizadas oscila entre el 17,43% de esta última y casi el 22% de la citada en primer lugar. El resto de los sectores, cuya incidencia en el total de actuaciones es inferior al 10%, son las siguientes:

- Administración Pública.
- Comunicaciones electrónicas comerciales – *spam* (LSSI).
- Profesionales, comunidades de propietarios, administración de fincas.
- Servicios de Internet.
- Comercio, transporte y hostelería.
- Sanidad.
- Recursos humanos, asuntos laborales, mutuas.

- Asociaciones, federaciones, colegios profesionales, ONG's, fundaciones, clubes.
- Suministro y comercialización de gas, electricidad y agua.
- Publicidad y prospección comercial (excepto *spam*).
- Informaciones publicadas en medios de comunicación.
- Seguros.
- Enseñanza.
- Fuerzas y cuerpos de seguridad.
- Envío de comunicaciones comerciales por fax (LGT).
- Sindicatos.
- Partidos políticos.
- Seguridad privada.
- Procedimientos judiciales.

Sin embargo, en las resoluciones de procedimientos sancionadores a entidades privadas, el sector de las telecomunicaciones y las entidades financieras, pese a ocupar el primer y tercer lugar por número de procedimientos, han descendido en un 10,34% y un 21,26% respectivamente.

Por el contrario, el sector de la videovigilancia privada por razones de seguridad asciende al segundo lugar del número de procedimientos sancionadores resueltos, con un crecimiento del 229,55% sobre el año anterior. Estas cifras confirman la afirmación de la Memoria de 2008 sobre que estamos ante un fenómeno omnipresente ante el que es preciso reforzar las garantías de los ciudadanos.

Se producen descensos significativos, superiores al 20%, de resoluciones sancionadoras en los sectores de comercio, transporte y hostelería y en el sector sanitario. El primero de ellos es relevante por tener un peso relevante las pequeñas y medianas empresas y el segundo por afectar a datos especialmente protegidos como son los de salud. Si bien en este último se aprecia un incremento de las solicitudes de tutela de derechos relacionadas con el acceso a la historia clínica.

Las resoluciones declarativas de infracción de la LOPD por las Administraciones Públicas crecen al mismo ritmo que las del sector

privado (en torno al 12,5%). En las Administraciones Autonómicas el incremento anual sigue siendo superior al 30% (38,10%), reduciéndose las relacionadas con la Administración General del Estado (-19,05%) y la Administración Local (-31,25%). Y pasan a tener un peso relativo cercano al 25% del total de resoluciones las infracciones cometidas por otras entidades de derecho público.
Las principales infracciones declaradas son:

- Infracciones del deber de secreto.
- Falta de medidas de seguridad, incluidos los hallazgos de documentación accesibles en la vía publica o en la basura.
- Tratamiento de datos con conculcación del principio de calidad de datos.
- Omisión del deber de información.
- Creación de ficheros sin disposición general habilitante y no inscripción en el RGPD.
- Cesión ilícita de datos.

Ahora bien, en valores absolutos, las infracciones de las Administraciones públicas se mantienen en niveles reducidos (71 frente a 621).

Las principales actuaciones inspectoras por iniciativa del Director de la AEPD han sido:

- Documentos con datos de carácter personal hallados en contenedores de basura en la vía pública procedentes de una agencia de seguros y un bingo catalán.
- Documentos abandonados en los locales de antigua comisaría de policía.
- Cámaras de videovigilancia instaladas por los vecinos en un barrio barcelonés.
- Documentos al alcance de los ciudadanos en el Registro Civil de Madrid.
- Almacenamiento de diversa documentación clínica en áreas no restringidas al público de un hospital psiquiátrico orensano.
- Portales de contactos personales que facilitan la votación de la imagen física de los usuarios, en particular cuando son menores de 14 años.
- Portal de contactos personales con usuarios de todo el mundo, clasificados según país (en particular, España) y centro educativo.
- Hallazgo por la Inspección de Datos en la red eMule de un fichero conteniendo datos de más de 3.000 clientes de una clínica canaria.
- Comunicación de datos de clientes entre dos filiales de un grupo empresarial de telecomunicaciones.
- Procedimiento de requerimiento telefónico del pago de deudas por parte de una entidad financiera.
- Revelación pública a través de los medios de comunicación de la identidad de una menor antes de su muerte, relacionada con unas actuaciones judiciales iniciadas como consecuencia de su hospitalización previa en un centro sanitario de Canarias.
- Análisis de la adecuación de un fichero común con información sobre inquilinos morosos.
- Análisis de la adecuación de los tratamientos realizados por una compañía especializada en servicios de *listbroking* en el sector del marketing directo.
- Formularios del Registro Central de Medidas Cautelares (Ministerio de Justicia).

El importe de las sanciones impuestas ascendió a 24.872.979,72 €. Aunque esta cifra supone un incremento del 12,99% sobre el año anterior, se aproxima al volumen de sanciones declaradas en el año 2006. (24.422.292,98 €).

Con la relevante diferencia de que el número de procedimientos sancionadores resueltos en 2009 es superior en un 235% al del 2006. (709 frente a 301).

Es precisamente el importante incremento de los procedimientos sancionadores y no la cuantía de las sanciones declaradas la que explica la cifra de sanciones impuestas.

De las resoluciones sancionadoras, el 92,84% se declaran en aplicación de la LOPD, el 5,76% en aplicación de la LSSI –con una disminución próxima al 5%- y el 1,40% en aplicación de la LGT.

Las sanciones que presentan un incremento mayor son las calificadas como leves (Δ44,76%), mientras que las sanciones graves permanecen estables y las muy graves disminuyen casi en un 6%.

El número de casos en que se apreció una disminución cualificada de la responsabilidad de los infractores fue del 40,72% del total de resoluciones sancionadoras. Los criterios aplicados para apreciar esta circunstancia fueron los siguientes:

- Cuando la entidad imputada ha absorbido o se haya fusionado con la entidad responsable que originó la infracción y no ha transcurrido un periodo prolongado.
- Cuando la entidad imputada dispone de un protocolo de actuación adecuado en la recogida de datos y tal protocolo haya, excepcionalmente, fallado.
- Cuando la entidad imputada ha regularizado la situación denunciada de forma diligente en un tiempo prudencial desde el conocimiento de los hechos.
- Cuando los hechos denunciados deriven de un error de difícil detección (no producido por una actuación negligente ni por la errónea aplicación de una norma).
- Cuando los hechos denunciados deriven de la falta de diligencia en la conducta del afectado o sea corresponsable de la infracción imputada a la entidad.
- Cuando quede acreditada la confianza legítima y no quepa la exoneración al obedecer la infracción a un requerimiento de la Administración.
- Cuando se trata de una persona física o pequeña o mediana empresa y la infracción se deba a cuestiones de cualificación técnica.

Por su parte las resoluciones de archivo y las denuncias inadmitidas se incrementaron en 15,83% y en un 450,14%, respectivamente. Los motivos más frecuentes de archivo fueron:

- Inaplicabilidad de la LOPD por estar excluido de su ámbito territorial de aplicación.
- Tratarse de un supuesto de cesión de deuda sobre la que ya ha recaído sanción.
- Incompetencia de la Agencia en la interpretación de cláusulas contractuales de orden civil/mercantil.
- El afectado o denunciante está excluido de la LOPD como persona jurídica.
- Tratamiento de datos relativos a fallecidos no amparados por la LOPD.
- Falta de indicios mínimos para abrir una investigación que invertiría el principio *in dubio pro reo*.
- Prevalencia del derecho a la libertad de expresión en medios de comunicación.
- Prevalencia del derecho a la tutela judicial efectiva como habilitante para el tratamiento de datos.
- Resultar procedente instar previamente la cancelación o rectificación al tratarse de una opción contemplada en el ordenamiento y no haberse producido daños.

Analizando los datos que se han expuesto cabe concluir que el incremento cuantitativo de las sanciones, consecuencia del incremento previo de las denuncias, no es obstáculo para apreciar una mejora en el cumplimiento de la LOPD, al crecer los incumplimientos por motivos formales, reducirse las infracciones muy graves y diminuir la culpabilidad cuando se comete una infracción.

La Memoria de 2008 recogió la preocupación ciudadana sobre la recepción de publicidad telefónica, constatada en la inspección sectorial realizada por la AEPD. En ella se citaban, entre otros problemas, los relacionados con el desconocimiento o la ausencia de procedimientos efectivos para oponerse a recibir publicidad.

La necesidad de dar una respuesta eficaz a esta cuestión ha llevado a la Agencia a promover, junto con la Federación Española de Comercio Electrónico y Marketing Directo (FECEMD), la puesta en marcha de un nuevo fichero de exclusión para evitar que quienes no desean recibir publicidad puedan manifestarlo.

El servicio de Lista Robinson, presentado conjuntamente el 30 de junio, ofrece las siguientes ventajas:

- Permite a los ciudadanos gestionar la publicidad que reciben.
- En particular, permite a los padres o tutores solicitar que no se traten los datos de los menores para el envío de publicidad.
- Posibilita elegir los canales a través de los que se desea recibir publicidad, incluyendo el postal, el correo electrónico, los mensajes SMS y MMS y el telefónico.
- En cada uno de los canales permite seleccionar varias opciones sobre la identidad de la persona, sus domicilios, las direcciones de correo electrónico y los números de teléfono.

El servicio de Lista Robinson es gratuito para quienes se registran, siendo efectiva la inclusión a partir de los tres meses del registro.

Este servicio no es aplicable a los casos en que la persona ha facilitado voluntariamente su consentimiento a entidades para que le envíen publicidad. No obstante, para la publicidad telefónica, que es una de las que generan mayor rechazo, ofrece una plataforma a los ciudadanos para revocar su autorización enviando un modelo de correo electrónico a las empresas adheridas al servicio de Lista Robinson. Para ello se ofrece una opción de búsqueda de las entidades adheridas.

Conforme al RLOPD, las empresas que realicen campañas publicitarias con los citados datos han de consultar previamente la Lista Robinson a fin de excluir a quienes no desean recibir publicidad.

De la información solicitada a FECEMD el número de personas registradas en el servicio de Lista Robinson ascendía a más de 110.000, a 31 de diciembre de 2009.

De ellos, un 37,75% no desea recibir publicidad telefónica, en torno al 25% rechazan mensajes SMS, un 23,23% se oponen a la recepción de correos electrónicos y un número más reducido (16,4%) no desean publicidad postal.

La puesta en marcha del servicio es una muestra palpable de la eficacia de las políticas preventivas y de colaboración con los obligados por la LOPD para incrementar las garantías de los ciudadanos.

En el ámbito de la actividad publicitaria, la Memoria de 2008 informaba, además, sobre la inspección sectorial realizada por la Agencia sobre los mensajes publicitarios y comerciales a telefonía móvil, sintetizando las principales deficiencias detectadas.

En 2009 se han producido avances en éste ámbito.

La Orden ITC/308/2008, de 31 de enero, que regula estos servicios estaba condicionada a la aprobación de un código de conducta para su prestación; el cual ha sido publicado por Resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en el Boletín Oficial del Estado de 27 de julio de 2009.

Con ello se ha dado respuesta a algunas de las recomendaciones de la inspección sectorial, entre las que destacan las siguientes:

- Identificación de los distintos servicios de tarificación adicional a través de los números que tienen asignados.

- Se establecen los requisitos que deberá reunir la información y la publicidad que se realice sobre los servicios de tarificación adicional basados en el envío de mensajes. Así cualquier publicidad que se realice de un número de tarificación adicional deberá informar al usuario del precio final y completo, impuestos incluidos y el contenido del servicio deberá ajustarse a lo publicitado.

- La obligación del operador titular del número que suministra los servicios de tarificación adicional de que sea fácilmente identificable para que los usuarios puedan ponerse en contacto con él y de informar al usuario de los servicios prestados, su precio y demás condiciones de contratación.

- La obligación de los operadores que facturan al abonado de informar a los usuarios sobre el derecho a la desconexión.

- Los operadores que provean el acceso al servicio deberán garantizar el derecho a la desconexión efectiva y evitar que la disconformidad del abonado con la facturación de los servicios de mensajes no dé lugar a la suspensión del servicio telefónico, ni del general de mensajes, si el abonado paga el importe de estos últimos.

En un entorno de crisis económica como el que se desarrolló durante 2009 con un alto crecimiento de la morosidad, se ha producido un incremento exponencial de actuaciones en materia de protección de datos derivadas o relacionadas con la reclamación de impagos.

Así, debe reseñarse el muy importante aumento en la invocación por los ciudadanos de los mecanismos de defensa otorgados por la LOPD frente a un indebido tratamiento de sus datos personales en la esfera de la morosidad. El número de tutelas iniciadas en tal materia se incrementó un 570% y el de actuaciones previas a un eventual procedimiento sancionador un 225%.

En el ámbito de cesión de cartera entre empresas (venta de deuda) se han resuelto varios expedientes sancionadores que han derivado en la imposición de sanciones que han llegado hasta 420.000 €. Se trataba de casos en que empresas, principalmente adscritas al sector de telecomunicación, realizaban la venta de la cartera de deudores a un cesionario que se encargaría de gestionar el recobro de deudas referentes a miles de clientes. Tras la comprobación de que en varios supuestos se estaba realizando la cesión de un deudor o deuda inexistente se adoptaron las decisiones sancionadoras citadas.

Otro problema suscitado ha sido el de la actualización de los domicilios del moroso para poder recabar la deuda correspondiente. En este sentido deben resaltarse las sentencias de la Audiencia Nacional que reconocen la obligación del deudor de mantener actualizadas sus señas permitiéndose en caso contrario su reactualización sin que se produzca vulneración de la LOPD. Junto a ello es significativa la inmovilización de un fichero de domicilios correspondiente a 36 millones de españoles utilizado con frecuencia para reactualizar los datos de los eventuales morosos pero alimentado por determinadas fuentes no conciliables con las previsiones de la normativa de protección de datos.

La entrada en vigor del Reglamento de desarrollo de la LOPD ha supuesto el inicio en la presentación de denuncias por vulneración de previsiones introducidas por la citada norma. Así ha ocurrido en lo relativo a la inclusión en ficheros de solvencia de referencias a deudas sobre las que se había entablado reclamación judicial, arbitral o administrativa, o bien sin especificar en el requerimiento previo a la inclusión que en el caso de no producirse el pago podrían ser comunicados los datos de impago a ficheros de solvencia o por haber accedido a la información contenida en el fichero sin tratarse de terceros habilitados.

Finalmente cabe reseñar varias denuncias frente a eventuales prácticas vulneradoras del deber de secreto en las actuaciones de recobro mediante la divulgación de la deuda existente a familiares o allegados al objeto de forzar el cobro de una cuantía supuestamente debida.

En relación con la conservación de los datos de salud está adquiriendo una importancia creciente dar respuesta a la cuestión de quién debe responsabilizarse de la custodia de las historias clínicas en los casos en que una entidad privada deja de prestar sus servicios o un profesional sanitario que ejerce privadamente su actividad se jubila o fallece.

En tales supuestos, de no existir una nueva entidad o profesional al que deseen acudir los pacientes, es preciso garantizar el cumplimiento de la obligación de conservación que impone la normativa sanitaria y, con ello, la disponibilidad para los ciudadanos de una información tan sensible como es la de su historia clínica.

Una alternativa factible sería potenciar que los Colegios Profesionales arbitrarán mecanismos para custodiar la información clínica a ante estas eventualidades.

3. LA PRIVACIDAD EN RIESGO: LOS GRANDES INTERROGANTES

A. INTERNET. NUEVOS SERVICIOS, NUEVOS RETOS

La oferta de servicios en Internet tiene en muchos casos un elemento común: la gratuidad para el usuario. El modelo de negocio que permite el acceso gratuito a estos servicios se basa en la publicidad asociada a ellos. Sin publicidad no existiría Internet tal como hoy lo conocemos.

El desarrollo de la publicidad en Internet se basa en un conocimiento cada vez más profundo de los hábitos del usuario con el fin de personalizar y hacer más eficaz el impacto del mensaje publicitario.

Las condiciones de uso del servicio se establecen unilateralmente por el prestador del mismo y el usuario se adhiere a ellas. La autorización del usuario para configurar perfiles de navegación o analizar el contenido de sus comunicaciones y recibir publicidad es la contraprestación por el uso gratuito de los servicios.

En este marco, la protección de la privacidad debe buscar nuevos caminos. La política reactiva basada en la declaración de infracciones y la imposición de sanciones es insuficiente. Deben primar las políticas activas de relación con los proveedores de estos servicios para que el diseño de los servicios y sus condiciones de uso ofrezcan garantías sobre el tratamiento de la información personal.

En 2009 la Agencia ha ampliado la política de interlocución con los prestadores de servicios, iniciada en relación con los motores de búsqueda, a otros servicios de uso masivo como las redes sociales en Internet.

Para conocer los riesgos para la privacidad y seguridad en las redes sociales la Agencia realizó junto con el Instituto Nacional de Tecnología de la Información (INTECO), un estudio sobre "la privacidad de datos personales, y seguridad de la información en redes sociales". El estudio incluye un catálogo de recomendaciones dirigidas a los responsables de estos servicios y a los propios usuarios, entre los que destacan las siguientes:

- Las condiciones de uso y políticas de privacidad deben redactarse con un lenguaje comprensible, para que cualquier tipo de usuario conozca sus derechos y obligaciones.
- Control de la indexación y almacenamiento de los perfiles por parte de los buscadores en Internet.
- Cambios en la configuración del nivel de privacidad, de forma que se establezca, por defecto, el máximo grado de seguridad en el perfil del usuario (generalmente permite la máxima difusión de los perfiles).
- Puesta a disposición del usuario de herramientas que le otorguen el control absoluto de la información que publica en la red; es decir, medios que limiten la posibilidad de etiquetar a otros usuarios en la red (recibiendo automáticamente una solicitud de aceptación o rechazo).
- Implantación de sistemas que faciliten la comprobación de la edad de los usuarios que intenten acceder al servicio, reduzcan los casos de suplantación de identidad (bloqueando el acceso al usuario que utilizó el perfil de otro de forma ilegítima) o detecten el nivel de seguridad de las contraseñas elegidas (e informen de los mínimos aconsejables).
- No publicar informaciones de terceros sin su consentimiento.
- No publicar en los perfiles excesiva información personal y familiar (ni datos que permitan la localización física), tener especial cuidado a la hora de alojar contenidos gráficos y configurar cuidadosamente el grado de privacidad del perfil de usuario en la red social.
- No aceptar solicitudes de contacto de forma compulsiva, sino únicamente a personas conocidas o con las que haya relación previa.

La Agencia trasladó a los responsables de algunas de las principales redes sociales que operan en España, Tuenti y Facebook, las recomendaciones del estudio, haciendo especial hincapié en la mejora de las políticas de privacidad para que ofrezcan una información clara, accesible y comprensible; en la necesidad de configurar políticas de privacidad por defecto, es decir en ausencia de una decisión del usuario, que garantice el máximo grado de privacidad y en la cancelación de todos los contenidos del perfil, en el momento en que se solicita la baja.

Las compañías han manifestado una disposición positiva para incorporar las mejoras y seguir manteniendo un dialogo fluido que permita evaluar los avances implantados.

La interlocución con los prestadores de servicios debe compatibilizarse con la resolución de las reclamaciones de los ciudadanos, cada vez más frecuentes.

El número total de expedientes de actuaciones previas iniciados en 2009 que se relacionaban más específicamente con servicios prestados a través de Internet fue de 156, lo que supone casi un 4% del total de actuaciones iniciadas en el ejercicio.

Como novedad más sobresaliente, 18 de esos expedientes (más del 11 %) se abrieron como consecuencia de 31 denuncias relacionadas con usuarios de las redes sociales Facebook y Tuenti, la mayor parte de las cuales se referían a la difusión de fotografías de terceros sin el consentimiento de éstos. Un aspecto destacable de estos expedientes es que las infracciones se imputan a los propios usuarios de los servicios y no a la empresa que lo presta, lo cual no es, en principio, responsable de los contenidos incorporados por los usuarios.

La mayor parte del resto de actuaciones tienen también relación con la difusión no autorizada de datos de carácter personal a través de Internet. 37 de ellas (casi 24 % del total) se refieren específicamente a foros o blogs, 13 (más del 8 %) a portales de video, fundamentalmente Youtube, y 38 (más del 24 %) a otro tipo de sitios web como sedes corporativas, repertorios jurídicos o páginas personales.

28 reclamaciones (un 18 % aproximadamente) se refiere a sitios web de anuncios, a portales de contactos personales o a servicios de correo electrónico. En su mayor parte se relacionan con la difusión no autorizada de datos.

10 de las actuaciones (más del 6%) se refieren a incidencias de diversa índole relacionadas con tiendas virtuales o, en general, con operaciones de comercio electrónico.

Son finalmente reseñables las 5 actuaciones previas iniciadas en relación con los servicios de búsqueda de páginas web y de localización de información personal en directorios o en buscadores de personas.

B. LOS MENORES. UNA PROTECCIÓN NECESARIA ANTE SU PRESENCIA CRECIENTE EN LA RED

El uso de redes sociales por parte de los menores se ha convertido en una actividad habitual para su desarrollo social. Esta actividad les reporta grandes ventajas al ofrecerles acceso a un nuevo medio de comunicación y de relación social. Los riesgos para los menores parten en gran medida de un déficit educacional básico: desconocen cómo ejercer un verdadero control sobre su información.

La normativa de protección de datos no permite a los menores de catorce años registrarse como usuarios de una Red social sin el consentimiento de sus padres. La Agencia ha asumido como una prioridad el cumplimiento de esta obligación.

En las reuniones mantenidas con los responsables de Tuenti y Facebook el control del acceso de los menores ha sido una exigencia permanente, analizando los procedimientos tecnológicos y organizativos que permitan hacerlo efectivo.

En abril de 2009 Tuenti adquirió el compromiso de implantar en el plazo de tres meses sistemas efectivos de verificación de la edad y a depurar los perfiles de los menores de catorce años registrados en la red social.

En el mes de julio Tuenti presentó a la AEPD las medidas adoptadas. La red social analiza los perfiles de usuarios que aparentan ser menores de catorce años y les envía una solicitud para que aporten fotocopia de su DNI o pasaporte en el plazo de 92 horas. Si no se recibe respuesta se comunica al usuario que su perfil será borrado.

Tuenti ha comprobado varios miles de registros sospechosos y ha borrado los perfiles en un porcentaje superior al 90% de los usuarios requeridos por la compañía. Tuenti se ha comprometido a reforzar los procesos de depuración de los perfiles existentes y a desarrollar sistemas de comprobación de los nuevos perfiles que se creen sospechosos de ser de menores de catorce años.

Asimismo informó sobre la modificación de la política de privacidad de la Red social, estableciendo por defecto el máximo nivel de privacidad –sólo entre amigos- para los menores de dieciocho años.

En Facebook la edad mínima para que los menores puedan ser usuarios de la red social son trece años, por ser la prevista en la legislación de los Estados Unidos de Norteamérica.

La Agencia instó a los responsables de la Red a que incrementaran la edad a los catorce años para los usuarios desde España. Posteriormente se reiteró el requerimiento solicitando información sobre el aumento de la edad y sobre los motivos que, en su caso, lo impidieran.

La preocupación por el control de los menores de catorce años ha sido compartida por el Defensor del Pueblo al que la Agencia ha informado sobre la evolución de las medidas adoptadas.

Más allá de las redes sociales, otros servicios en Internet también presentan riesgos para los menores, entre los que destacan los portales de contactos en los que se publican imágenes, en ocasiones provocativas, de adolescentes y se facilita la votación sobre ellas.

La creciente presencia de los menores como usuarios de Internet hace necesario completar las acciones que se han descrito, con un impulso decidido para incorporar a los planes de estudio una formación adecuada sobre protección de datos y privacidad, así como para que las Administraciones Públicas y los centros educativos pongan a disposición de los alumnos tecnologías que limiten el acceso a servicios de la Red a los menores de catorce años.

En esta búsqueda de herramientas para verificar la edad de los menores, el Documento Nacional de Identidad electrónico, por medio del certificado reconocido de autenticación, se revela como uno de los instrumentos más eficaces para acreditar la edad en Internet.

Por ello, esta Agencia considera extraordinariamente importante que se pongan en marcha las iniciativas adecuadas con el fin de que los mayores de catorce años dispongan de los medios digitales que permitan acreditar que tienen la edad requerida para otorgar su consentimiento para el tratamiento de sus datos.

Esta iniciativa posibilitaría que la industria relacionada con las redes sociales y otros servicios disponibles en Internet adaptasen sus aplicativos con el fin de permitir la identificación de los menores.

C. LA VIDEOVIGILANCIA: CONVIVIR CON GARANTÍAS

La videovigilancia por razones de seguridad se ha convertido en una realidad omnipresente. Cada año se produce un crecimiento significativo de los ficheros de videovigilancia, especialmente, por parte de entidades privadas, aunque también por las Administraciones Públicas. Los ficheros inscritos en el Registro General de Protección de Datos que declaran esta finalidad se incrementaron en torno al 240% en el ámbito privado superando la cifra de 37.000.

Los principales sectores en los que se declaran ficheros de videovigilancia son el comercio, con una quinta parte del total, seguido del turismo y hostelería, las comunidades de propietarios, la sanidad, la industria química y farmacéutica, la construcción y las actividades relacionadas con los productos alimenticios, bebidas y tabaco. Todos ellos con una cifra superior al millar de ficheros.

En el ámbito público el incremento fue del 60% con un total de 578 ficheros.

De lo que se desprende que la videovigilancia se ha convertido en una realidad de nuestra vida cotidiana con el que es necesario convivir. Pero convivir con garantías para la privacidad.

La encuesta del CIS de 2009 refleja cómo perciben esa convivencia los ciudadanos, destacando los siguientes parámetros:

- La mayoría de los encuestados se sitúan en una posición intermedia si tienen que elegir entre libertad y seguridad.
- En cuanto a las cámaras de videovigilancia, el 68,7% se muestra a favor de su colocación. De ellos, el 66,4% lo apoyan porque proporciona más seguridad, el 18,0% porque permite la identificación de los delincuentes y el 15,2% porque evita delitos.
- En contra de la instalación de cámaras se posiciona el 10%. El motivo fundamental para posicionarse en contra es la pérdida de intimidad con un 79,4%.
- El 43,8 % ve muy bien y el 51,7% ve bien la instalación de cámaras en bancos. En comercios le parece muy bien al 34% y muy bien al 54.3%. En guarderías y colegios le parece bien al 50,6 % y muy bien al 26,6%.
- Los lugares donde son menos partidarios los ciudadanos a la instalación de cámaras son los locales de trabajo, en los que le parece mal o muy mal al 36,7 %, y bares y restaurantes, donde le parece mal o muy mal al 36%.
- Respecto a la señalización de las cámaras el 62,2 % sabe que debe señalarse su instalación y el 7% cree que no deben señalarse.
- El 72,8% se muestra a favor de que se controle la difusión de imágenes grabadas por cámaras de videovigilancia que se emiten por televisión o Internet. El 15% se muestra en contra.
- Los casos de difusión de imágenes por Internet o televisión en los que se ha vulnerado el derecho a la intimidad le parece bastante preocupante al 46,0% y le preocupa mucho al 26,9%.

No obstante la percepción que se desprende de la encuesta del CIS debe ser matizada por el hecho de que cada vez es mayor el número de personas que denuncian incumplimientos de la LOPD en relación con la videovigilancia, en la que se han incrementado en un 230 % los procedimientos sancionadores resueltos.

Las denuncias presentadas se refieren a la instalación de cámaras de videovigilancia realizadas por particulares, para vigilar viviendas unifamiliares, instaladas en garajes comunitarios, en la ventana de sus viviendas o para vigilar servidumbres de paso. También afectan a la instalación de cámaras en empresas o entidades tanto públicas como privadas sin cartel informativo sobre la videovigilancia.

Otro grupo de denuncias son a empresas que han utilizado las imágenes grabadas por las videocámaras para aportarlas en juicios, como mecanismo probatorio en la imposición de sanciones disciplinarias o para el despido de trabajadores.

Por lo que cabe concluir que la percepción positiva sobre la videovigilancia va acompañada de una exigencia de garantías para la privacidad. En definitiva: una convivencia con garantías.

Ante esta situación cobran especial relevancia las políticas activas de información a los responsables de estos ficheros y a los ciudadanos.

En este sentido la Agencia incluyo la videovigilancia como tema central de la II Sesión Anual Abierta celebrada el Día Europeo de Protección de Datos, y presentó una guía sobre la misma. La guía de videovigilancia es un documento conciso y accesible que pretende ofrecer indicaciones y criterios prácticos que permitan un adecuado cumplimento de la legislación vigente en la captación y tratamiento de datos con dicha finalidad.

Por otra parte, la reciente promulgación de la Ley 25/2009, de 27 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios, ha venido a ampliar la legitimación para la instalación y uso de dispositivos de videovigilancia. Lo que presumiblemente dará lugar a una reducción de las resoluciones sancionadoras de la AEPD, al ser dicha falta de legitimación una de las infracciones más frecuentes.

El uso de videocámaras, dada la accesibilidad de la tecnología y la reducción de costes, se ha generalizado para otras finalidades distintas de la seguridad.

Entre estas actividades se incluye la instalación de cámaras accesibles a través de Internet con diversas finalidades como son la captación de imágenes panorámicas de paisajes, la captación de imágenes en la vía pública, en el lugar de trabajo, en establecimientos comerciales o en vestíbulos de hoteles.

En todos estos casos se trata de cámaras conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de imágenes en tiempo real.

La AEPD realizó de oficio una inspección sectorial sobre el empleo de cámaras que permiten difundir imágenes a través de Internet con el fin de obtener conclusiones sobre el respeto a las garantías que la LOPD reconoce a los ciudadanos.

En la inspección se ha constatado que en muchos casos las cámaras que emiten imágenes a través de Internet únicamente recogen paisajes o panorámicas en los que, al no recabar imágenes de personas o recabarlas de forma que no puedan ser identificadas o reconocidas, no presentan riesgo para la privacidad. Sin embargo, la mayor parte de las cámaras permiten la identificación de las personas captadas.

La principal deficiencia que se ha constatado es que, aunque las cámaras disponen de mecanismos de control para el acceso a las imágenes basados en usuario y contraseña que evitarían el acceso indiscriminado a través de Internet, es habitual que dichos mecanismos estén desactivados por el fabricante o estén activados con usuario y contraseña por defecto, fácilmente identificable para cualquier usuarios de Internet. A lo que se une una falta de diligencia por las personas o entidades que instalan las cámaras, que no activan dichos controles o no modifican los incorporados por defecto, creando una vulnerabilidad que permite el acceso por terceros al dejar la cámara en una situación de "puertas abiertas".

Estas deficiencias permiten, en ocasiones, no sólo acceder al visionado de las imágenes, sino incluso manejar remotamente la cámara a través del "zoom", moviéndolo en sentido vertical u horizontal, obteniendo sonido o grabando las imágenes recibidas.

Este riesgo se multiplica como consecuencia de las facilidades que ofrecen los buscadores en Internet para obtener información sobre los procedimientos de acceso a las cámaras.

En cuanto a la titularidad de las cámaras instaladas se ha constatado que no sólo son propias de empresas, sino también de personas físicas.

Como consecuencia de la inspección se ha elaborado un catálogo de recomendaciones entre las que destacan los siguientes:

- Es esencial activar el control de acceso a las imágenes con usuario y contraseña y formar al personal que las utiliza.
- Recordar tanto a particulares como a empresas que la utilización de videocámaras para vigilar la vía pública está reservada únicamente a las Fuerzas y Cuerpos de Seguridad del Estado.
- Si capta imágenes panorámicas, -paisajes, edificios, tráfico urbano etc.-, asegúrese de que nunca se tomen planos cercanos que muestren rasgos reconocibles y evite que terceros no autorizados accedan a los controles de la cámara.
- Si se emplean cámaras de video conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de las imágenes en tiempo real para el control de la actividad de los trabajadores, deben ser informados y respetarse sus derechos. Si se van a difundir imágenes de una empresa con fines promocionales es necesario obtener el consentimiento de los empleados.
- Asegúrese de que si los menores utilizan webcam para realizar videollamadas, chat con video o mostrar imágenes en tiempo real a amistades, lo hacen de forma segura y controlada y compruebe que los menores realizan un uso apropiado, bajo su supervisión de las webcam.
- Asimismo, se incluye como recomendación a los fabricantes y distribuidores de estos dispositivos que faciliten, junto con la documentación o instrucciones, el Decálogo para usuarios de videocámaras conectadas a Internet.

Como consecuencia de la inspección se han iniciado y resuelto siete procedimientos sancionadores.

D. ENTORNO LABORAL: EQUILIBRIO ENTRE DERECHOS Y OBLIGACIONES

La variedad de tratamientos de datos personales que se llevan a cabo en el entorno laboral ha motivado que la AEPD tomara la iniciativa de elaborar una guía sobre la protección de datos en la empresa. La guía se plantea, así, con el objetivo de ofrecer respuesta a un conjunto de aspectos prácticos a los que las empresas deben enfrentarse habitualmente, sugiriendo los criterios que permitan cumplir la normativa de protección de datos personales. Con el efecto añadido de que pueda servir de punto de referencia en las relaciones entre los agentes sociales implicados.

En la gestión de recursos humanos la guía destaca la importancia de informar a los trabajadores sobre las finalidades para las que se utilizará la información diferenciando los tratamientos vinculados al contrato de trabajo de otras finalidades distintas.

Asimismo, se diferencian los usos de la información en los procedimientos de selección del personal, en la contratación y durante el desarrollo de la relación laboral.

Se incluyen recomendaciones específicas sobre el tratamiento de datos especialmente protegidos, en particular, los de salud y afiliación sindical, así como las garantías que deben observarse en la prevención de riesgos laborales por parte de los distintos sujetos que pueden intervenir en ella.

Aún no tratándose necesariamente datos personales, la guía incorpora recomendaciones para que la implantación de sistemas internos de denuncia en la empresa se lleve a cabo garantizando la protección de los empleados.

Destaca el capítulo dedicado a los controles empresariales que progresivamente alcanzan a un mayor número de aspectos de la relación laboral, indicando las reglas aplicables a controles biométricos, la videovigilancia en el trabajo o sobre el uso de las herramientas tecnológicas facilitadas por el empleador y, también, los relacionados con el control del absentismo laboral.

Las relaciones con los sindicatos se contemplan con una perspectiva amplia que comprende la publicación de datos personales en tablones y los accesos y cesiones de información a los sindicatos.

Y, concluye con un recordatorio a los trabajadores sobre sus deberes respecto a la seguridad y el secreto que deben presidir el uso de la información que conozcan en el marco de actividad laboral.

E. LOS FLUJOS INTERNACIONALES DE DATOS. FLEXIBILIDAD Y GLOBALIZACIÓN

Las transferencias internacionales de datos desde España se han globalizado y alcanzan todas las áreas geográficas del mundo. El número de autorizaciones se incrementó en un 25%. Los Estados Unidos (EEUU), pese a la disminución del número de transferencias, continúa siendo el primer país de destino.

Los países latinoamericanos presentan un fuerte crecimiento superior al 100% y se aproximan con un total de 132 autorizaciones a los volúmenes de EE.UU. Asia sigue manteniendo un volumen constante de autorizaciones alcanzando la cifra total de 115 debido, fundamentalmente, al fuerte impulso de la India como país importador con más de la mitad de las autorizaciones (67).

En el continente africano las transferencias internacionales se focalizan en Marruecos (19) y la Republica Sudafricana (3). Y Australia apunta como destino emergente con un fuerte crecimiento en 2009.

La brecha entre las transferencias de responsable a responsable y las que tienen como finalidad externalizar la prestación de servicios en terceros países sigue aumentando a favor de estos últimos que constituyen el 87,5% del total.

Las primeras se circunscriben prácticamente a la gestión administrativa de recursos humanos. En la deslocalización de servicios en terceros países los principales objetivos son la teleoperación y el alojamiento de información en servidores *hosting*.

Los principales exportadores de datos que solicitan autorización se concentran en los sectores bancario, asegurador y de telecomunicaciones.

El incremento creciente de los flujos internacionales de datos se aprecia, también, en los nuevos ficheros de titularidad privada inscritos en el RGPD, que declaran este tipo de operaciones sin estar sujetas a autorización. En 2009 han sido 539 los ficheros inscritos con un incremento del 25%.

Los principales sectores de actividad en que operan las entidades exportadoras de datos son telecomunicaciones, energía, servicios informáticos, banca, industria química y farmacéutica, y publicidad directa.

La búsqueda de procedimientos más flexibles para la autorización de transferencias internacionales ha avanzado en 2009. La AEPD autorizó la primera transferencia basada en cláusulas corporativas vinculantes (BCR) y ha participado a través de un procedimiento coordinado en diez solicitudes con esta modalidad de garantías presentadas ante otras Autoridades de la Unión Europea.

Los trabajos para adoptar una nueva Decisión de la Comisión que facilite la transferencia internacional de datos a prestadores de servicios y, especialmente, la subcontratación a terceros países, se ultimaron en 2009. La Decisión ha sido finalmente adoptada en febrero de 2010.

Como conclusión, puede afirmarse que asistimos a un incremento constante de flujos internacionales de datos con un gran peso de la deslocalización de servicios y con procedimientos más flexibles de autorización.

De lo que se desprende la urgencia de alcanzar unos estándares vinculantes para garantizar la protección de la privacidad en un mundo globalizado.

4. 2009. MADRID, CAPITAL MUNDIAL DE LA PRIVACIDAD. LA RESOLUCIÓN DE MADRID: UN PUNTO DE ENCUENTRO PARA UNA REGULACIÓN GLOBAL

La AEPD organizó en 2009 la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, el mayor foro dedicado a la privacidad a nivel mundial y punto de encuentro privilegiado entre autoridades de protección de datos y garantes de la privacidad de todo el planeta, así como de representantes de entidades públicas y privadas y de la sociedad civil. Durante una semana, en concreto la comprendida entre el 2 y el 6 de noviembre, España se convirtió en el centro mundial de la privacidad.

Con más de mil asistentes provenientes de 83 países, esta edición de la Conferencia ha sido la más concurrida en sus treinta años de historia, y la más exitosa en palabras de muchos de sus participantes. Inaugurada por SS.AA.RR. los Príncipes de Asturias, se desarrolló en el Palacio de Congresos de Madrid, bajo el lema "Privacidad: hoy es mañana". Entre los casi cien ponentes, repartidos en veinte sesiones, destacaron el ministro de Interior español, Alfredo Pérez Rubalcaba y la secretaria de Seguridad Nacional de los Estados Unidos, Janet Napolitano; Martin Cooper (Premio Príncipe de Asturias 2009 de Investigación Científica y Técnica e inventor del teléfono móvil), Vinton Cerf (Premio Príncipe de Asturias 2007 de Investigación Científica y Técnica y co-inventor de la familia de protocolos de Internet TCP/IP) y Adi Shamir (co-inventor del algoritmo de cifrado RSA), así como el ministro de Industria, Comercio y Nuevas Tecnologías de Marruecos, Ahmed Reda Chami.

Como en años anteriores, la Conferencia abordó aquellas cuestiones que, por su relevancia o novedad, formaron parte de la agenda internacional en materia de protección de datos. La evolución de Internet, la globalización y las nuevas técnicas publicitarias compartieron espacio con la seguridad, el periodismo ciudadano y la privacidad en el puesto de trabajo; temas, todos ellos, tratados desde una triple óptica: académica, económica y social.

No obstante, el mayor logro de esta edición se deriva de la consecución de su objetivo prioritario: avanzar hacia un instrumento legal, universal y vinculante en materia de privacidad, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado y que cuente con el más amplio consenso institucional y social. Mediante la adopción de la denominada "Resolución de Madrid", la Sesión Cerrada de la Conferencia acogió con satisfacción el primer gran paso en esta línea: la "Propuesta conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal", instó a todas las autoridades participantes a darle la máxima difusión a nivel tanto nacional como internacional, y marcó una estrategia para impulsarla y evaluar su difusión.

La Propuesta Conjunta pretende, por una parte, promover internacionalmente el derecho a la protección de datos y la privacidad, ofreciendo un modelo de regulación que garantice un alto nivel de protección y que, al mismo tiempo, pueda ser asumido en cualquier país, con las mínimas adaptaciones que sean necesarias en función de las diversas culturas jurídicas, sociales o económicas propias de cada región. Del mismo modo, la Propuesta busca facilitar el flujo de datos personales a nivel internacional, tratando de mitigar los obstáculos y retrasos existentes, que implican costes adicionales para las empresas y generan desequilibrios desde el punto de vista de la competencia.

Pese a no tratarse de un acuerdo internacional ni de una normativa jurídicamente vinculante, su valor y relevancia como texto de referencia se derivan de la amplia participación de la comunidad internacional de protección de datos y privacidad en su elaboración, de que recoge elementos que están presentes en todos los sistemas vigentes de protección de datos actualmente en vigor y de que ha sido respaldada por todas las Autoridades integrantes de la Conferencia Internacional. De este modo, la propuesta se configura no sólo como la base para la futura elaboración de un Convenio universal vinculante, sino como una herramienta de indudable utilidad para el desarrollo normativo e institucional en aquellos países en los que la protección de datos no se encuentre todavía convenientemente implementada.

Respondiendo al mandato contenido en la Resolución de Madrid, la promoción y difusión de este texto entre entidades privadas, expertos y organismos públicos nacionales e internacionales, será una de las prioridades de la AEPD durante el año 2010.

5. CLAVES PARA EL DESARROLLO DE UN NUEVO MARCO EUROPEO DE PRIVACIDAD

A. TRATADO DE LISBOA

El Tratado de Lisboa, firmado el 13 de diciembre de 2007, entró en vigor el pasado 1 de diciembre de 2009 tras su ratificación por todos los Estados miembros. Este Tratado incluye la Carta de los Derechos Fundamentales de la Unión Europea que reconoce, refuerza y hace vinculantes los derechos, libertades y principios de los Estados miembros de la Unión Europea. La Carta contiene dos artículos en materia de privacidad y protección de datos que marcan una importante consolidación de la legislación de protección de datos de la Unión Europea.

El Tratado de Lisboa, entre otras novedades, también extingue el sistema de pilares de la Unión Europea, creando un marco común para todas las actividades de la Unión aboliendo la antigua división. Este cambio de estructura se refleja también en el ámbito de la protección de datos. Hasta ahora, si bien la protección de datos gozaba de armonización en el ámbito del primer pilar de la Comunidad Europea con las Directivas 1995/46/CE y 2002/58/CE, no era así en las actividades llevadas a cabo en el marco del tercer pilar, el relativo a la cooperación policial y judicial en materia penal, donde la materia había sido regulada separadamente en virtud de una Decisión Marco adoptada en fecha tan tardía como 2008.

Además, marca la necesidad de una supervisión independiente y desarrolla instrumentos para proveer una mayor protección de datos de manera homogénea a través de las diferentes actividades de la Unión Europea, y con una mayor participación del Parlamento Europeo, también con respecto a los acuerdos internacionales.

El nuevo marco jurídico de la Unión Europea es un reto para las autoridades de protección de datos, que tendrán que revisar las normas en vigor y asesorar a los legisladores en la toma de decisiones en los nuevos campos de actividad.

B. PROGRAMA DE ESTOCOLMO

El programa de Estocolmo sobre el Espacio Europeo de Libertad, Seguridad y Justicia fue aprobado en la última reunión del Consejo de Ministros de la Presidencia Sueca de la Unión Europea, el 12 y 13 de diciembre. Con este Programa se fija la agenda de justicia e interior para los próximos cinco años, centrada en el terrorismo, la seguridad informática, la delincuencia organizada y el control fronterizo entre otros temas de interés y sustituye al anterior "Programa de la Haya", cuya vigencia expiró en diciembre.

En el Programa se reconoce la protección de los derechos fundamentales, y en particular, como uno de los aspectos clave, la protección de los datos personales. El Programa de Estocolmo asimismo establece que la UE debe contar con un único sistema de protección de datos personales que incluya un modelo de certificación europea para las tecnologías, productos y servicios que protejan la intimidad.

En la misma línea, la Conferencia Europea Autoridades de Protección de Datos, celebrada en Edimburgo en abril de 2009, llegó a la conclusión de la necesidad de revisar el marco europeo de protección de datos, y la necesidad de analizar la legislación en un mundo globalizado y en el que el uso de Internet y el desarrollo del comercio electrónico y gobierno electrónico se centra en la información personal.

C. FUTURO DE LA PRIVACIDAD

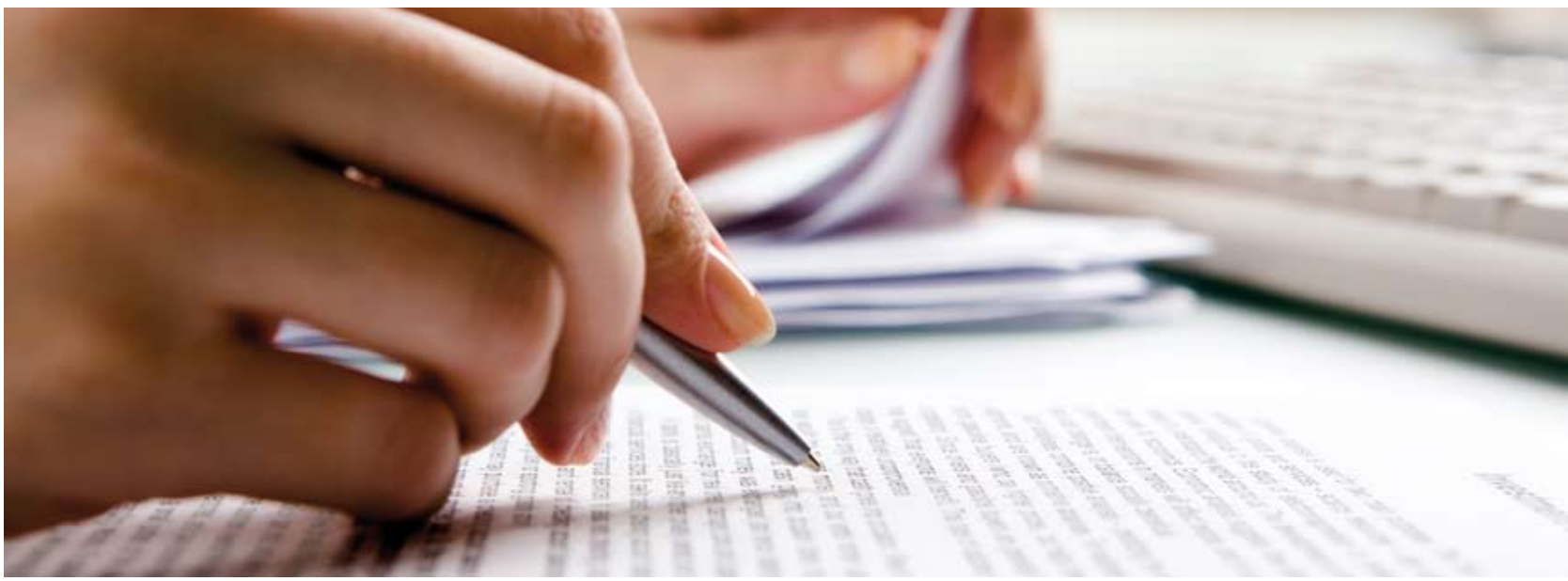
La previsible repercusión, sobre el marco legal europeo en materia de protección de datos, de la entrada en vigor del Tratado de Lisboa y del Programa de Estocolmo, se pone de manifiesto en la puesta en marcha por parte de la Comisión Europea de un ambicioso proyecto, encaminado a analizar los futuros avances en el desarrollo de este derecho fundamental. Ambos textos, unidos a la preocupación por el impacto que la globalización y las nuevas tecnologías están teniendo sobre la privacidad, serán piezas claves en este proceso, iniciado en

mayo mediante la celebración de una Conferencia en Bruselas: "Datos personales: ¿mayor uso, mayor protección?", al que siguió una consulta pública sobre el marco legal de este derecho fundamental.

Las Autoridades de Protección de Datos, que forman parte del Grupo de Trabajo del Artículo 29 han mostrado en todo momento su interés en participar activamente, como actor especialmente cualificado, en este proceso de consulta. Para ello, ha elaborado un documento que plasmara su posición ante los diferentes retos a que se enfrenta la protección de datos en Europa. En dicho documento, "Futuro de la Privacidad: Contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de datos personales", las Autoridades Europeas, y entre ellas la AEPD, coinciden en señalar que la validez de los principios básicos recogidos en la actual legislación en materia de protección de datos está fuera de toda duda, a pesar de los cambios institucionales, tecnológicos y sociales a los que estamos asistiendo. No obstante, también opinan que el marco jurídico actual puede ser mejorado en lo relativo a su aplicación práctica, en especial en lo tocante a los siguientes puntos:

- Clarificación de los conceptos y principios ya existentes, basada en la experiencia resultante de su aplicación.
- Introducción de nuevos principios, como la noción de privacidad desde el diseño *privacy by design*.
- Modernización de las disposiciones de la Directiva 95/46/CE, a los efectos de mejorar la efectividad en su aplicación práctica.
- Aplicación de los principios de la protección de datos a los asuntos relativos a la cooperación judicial y policial.
- Una definición más clara de los criterios establecidos para considerar que una transferencia internacional de datos se realiza ofreciendo las garantías adecuadas, prestando especial atención a la Propuesta Conjunta de Estándares Internacionales de Privacidad.

Con vistas a analizar las aportaciones recibidas como respuesta a la consulta de la Comisión, durante 2010 se convocará un grupo de expertos que emitirá un informe en el que expondrán las posibles mejoras que, en su opinión, deberían introducirse en la legislación comunitaria en materia de protección de datos.



6. RECIENTES DESARROLLOS INTERNACIONALES

A. REDES SOCIALES ONLINE

En el mes de junio, el Grupo de Trabajo del Artículo 29 (GT29) aprobó la Opinión sobre redes sociales on-line. La finalidad de esta opinión es establecer criterios para adaptar los servicios que operan de forma global a los requisitos de la legislación de protección de datos de la Unión Europea. Entre otras cuestiones, la Opinión distingue bajo qué circunstancias puede considerarse que los usuarios se encuentran en una mera actividad personal o familiar, y por tanto, no sujetos a las obligaciones en materia de protección de datos, o cuando pueden adquirir responsabilidad por la información publicada.

En ese sentido el GT29 ha considerado que no se aplicará la excepción doméstica y por tanto se aplicarán las leyes de protección de datos en las siguientes situaciones: Cuando la red social on-line se utilice como una plataforma de colaboración para una asociación o una empresa, o cuando el acceso a la información del perfil vaya más allá de los contactos elegidos. En particular, cuando todos los miembros que pertenecen a la red social puedan acceder a un perfil o cuando sea posible acceder a los datos usando motores de búsqueda, se considera que el acceso sobrepasa el ámbito. Por último, la aplicación de la exención doméstica se ve también limitada por la necesidad de garantizar los derechos de los terceros, especialmente por lo que se refiere a los datos sensibles en el ámbito personal o doméstico. En los casos en que la exención domestica no resulta aplicable, los propios usuarios pueden ser responsables por incumplimiento de la LOPD.

Por otro lado, el GT29 apunta que los proveedores de servicios de redes sociales y, en muchos casos, quienes desarrollan aplicaciones para ellas son responsables por los datos personales que manejan, y, en ese sentido, tienen una responsabilidad para con los usuarios. En este contexto, considera que deben aplicarse todas las medidas necesarias dirigidas a proteger de forma adecuada la información publicada en sus plataformas.

El documento incluye una serie de recomendaciones dirigidas a los proveedores, que están encaminadas a reforzar los derechos de los usuarios. Entre ellas, la prohibición de utilizar la información publicada para finalidades no previstas, o la necesidad de que los proveedores configuren la red para que los perfiles ofrezcan acceso limitado por defecto.

B. CÓDIGO DE PRIVACIDAD DE LA AGENCIA MUNDIAL ANTIDOPAJE

La elaboración, por parte de la Agencia Mundial Antidopaje (WADA-AMA), de unos estándares en privacidad y protección de datos destinados a cubrir los tratamientos realizados en la lucha contra el dopaje, fue otro de los asuntos abordados por el Grupo del Artículo 29. En su Dictamen 4/2009 realiza un segundo análisis de la adecuación al derecho comunitario de estos estándares, que ya habían sido sometidos al parecer del GT29 en verano de 2008, y que fueron aprobados sin recoger muchas de las preocupaciones manifestadas entonces por el Grupo de Trabajo.

El documento reconoce los esfuerzos realizados por WADA-AMA de cara a la mejora del texto, pero concluye que la versión finalmente adoptada requeriría de una serie de mejoras en aspectos como:

- La presumible falta de libertad de los deportistas a la hora de consentir el tratamiento de sus datos, en el marco de controles antidopaje.
- Los periodos de conservación de los datos de los análisis realizados.
- La inexistencia de un procedimiento eficaz de control del cumplimiento del estándar.

Tras una serie de reuniones, celebradas tanto en el seno del propio GT29 como a instancias del Consejo de Europa, WADA-AMA adoptó en el mes de mayo una nueva versión de sus estándares, incorporando gran parte de las sugerencias contenidas en el dictamen del GT29. Las diferentes mejoras introducidas, fruto de un arduo proce-

so de negociación fomentado por el Consejo Superior de Deportes, contribuyeron a su mejor adaptación a los niveles de protección exigidos por la normativa española y comunitaria, y en consecuencia a una mayor protección de los datos empleados para la prevención del dopaje a nivel global.

C. OPINIÓN SOBRE LA MODIFICACIÓN DE LA DIRECTIVA 2002/58/CE

El pasado 4 de noviembre, y tras años de negociaciones, se llegó a un acuerdo sobre la reforma del paquete de telecomunicaciones, que culminó con la aprobación de las Directivas 2009/136/CE y 2009/140/EC y el Reglamento (CE) Nº 1211/2009. Los Estados miembros tienen un plazo de 18 meses para su transposición.

De forma previa a la aprobación de la Directiva, el GT29 formuló el Dictamen 1/2009 sobre las propuestas que modifican la Directiva 2002/58/CE 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) en la que realizaba una serie de observaciones respecto de las Enmiendas del Parlamento, los comentarios de la Comisión y el Acuerdo del Consejo. El documento expresaba su inquietud sobre otros asuntos, como la notificación por infracciones de seguridad y su ampliación a los servicios de la sociedad de la información, tipos de infracciones que han de notificarse, personas a quien pueden notificarse esas infracciones o la afirmación de que los datos de tráfico están sometidos a la legislación sobre protección de datos.

La Directiva 2009/136/CE modifica las Directivas 2002/22/CE (Directiva sobre servicio universal) y 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), armonizando de esta forma las disposiciones necesarias para garantizar un nivel equivalente de protección de los derechos y las libertades fundamentales en los estados miembros y, en particular, del derecho a la intimidad y a la confidencialidad, en lo que respecta al sector de las comunicaciones electrónicas. Asimismo aboga por la adopción de medidas destinadas a garantizar que los equipos terminales estén fabricados de manera que protejan los datos personales y la intimidad, estando estas medidas obligadas a respetar el principio de neutralidad con respecto a la tecnología.

Además, la citada Directiva se aprueba reflejando en su articulado el espíritu cambiante de las nuevas tecnologías, dejando abierta la posibilidad de que en un futuro surjan nuevos retos. La Directiva realiza cambios sobre cuatro puntos, que se enumeran a continuación.

- Reforzar los poderes de *enforcement* para las autoridades de protección de datos nacionales.

- Seguridad: Obligación de notificar las violaciones de datos personales.

- Reforzar la protección contra la interceptación de las comunicaciones a través de la introducción de *cookies* o *spyware* en los ordenadores de los usuarios, así como la necesidad de prestar consentimiento informado para la introducción de "cookies".

- Posibilidad de que cualquier persona afectada por el envío de comunicaciones no solicitadas por vías electrónicas *spam*, incluyendo a los proveedores de servicios de Internet, pueda llevar a cabo medidas legales efectivas en contra de los responsables del envío de dichas comunicaciones.

D. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

La actividad de la Red Iberoamericana de Protección de Datos se ha centrado en el desarrollo de las líneas estratégicas marcadas en el VI Encuentro de 2008.

Desde el punto de vista organizativo en el mes de mayo se celebró en Cartagena de Indias una reunión del Comité Ejecutivo de la Red Iberoamericana y se ha diseñado el sitio web específico de la Red www.redipd.org, que está operativo desde noviembre de 2009.

El intercambio de información entre instituciones y empresas y la apertura de la Red a terceros países que no pertenecen al entorno iberoamericano se ha impulsado con la celebración en Cartagena de Indias del I Seminario Euro-Iberoamericano de Protección de Datos dedicado al análisis de los problemas relacionados con la protección de los menores.

Con ocasión del VII Encuentro Iberoamericano, la Red dio un salto cualitativo en sus relaciones institucionales con la celebración de una reunión conjunta con la Asociación Francófona de Autoridades de Protección de Datos a la que asistieron representantes de 26 países, así como de la Comisión Europea y del Supervisor Europeo de Protección de Datos.

El encuentro, que culminó con una declaración conjunta suscrita por la Red Iberoamericana y la Asociación Francófona, constituye un primer paso de colaboración entre organizaciones regionales que favorecerá la sensibilización y la cooperación en materia de protección de datos en un entorno globalizado.

La colaboración institucional se ha manifestado, adicionalmente, en la participación de la AEPD en el Sexto Seminario Nacional e Internacional celebrado en Buenos Aires bajo la rúbrica "la Protección de Datos personales: Éxitos e Innovaciones en el Bicentenario de la República Argentina", así como en las X Jornadas Académicas Internacionales que tuvieron lugar en Montevideo y en el lanzamiento de la Unidad Reguladora y de Control de Datos de Uruguay organizado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y Sociedad de la Información (AGESIC) de dicho país.

El desarrollo de acciones para promover la adopción de normas de protección de datos en países iberoamericanos y facilitar su adecuación en el ámbito europeo se ha traducido en la visita a la AEPD de una delegación del Gobierno y el Consejo de la Transparencia chilenos, de una delegación del Gobierno brasileño integrada por los Ministerios de Justicia, Interior y Economía y Hacienda y en un intercambio de informaciones con la Embajada de Guatemala en Madrid.

Junto a estas actividades el acontecimiento más relevante de participación de la Red Iberoamericana en la comunidad internacional de protección de datos y de la privacidad ha sido la celebración del VII Encuentro de la Red en las jornadas previas a la celebración de la 31 Conferencia internacional. Su convocatoria en Madrid ha permitido, por primera vez, mantener una presencia amplia de los países iberoamericanos en el más importante foro mundial sobre la materia. La presencia de estos países ha posibilitado su intervención en diversas sesiones de la Conferencia y ha supuesto un punto de apoyo en la promoción de la Propuesta de Estándares internaciones de protección de datos.

Esta presencia fuera del entorno iberoamericano se ha completado con la participación de la Red en calidad de observadora en las reuniones del Consejo Consultivo del Convenio 108 del Consejo de Europa a partir del mes de marzo de 2009.

Desde una perspectiva bilateral la Agencia ha participado en el debate sobre la interrelación entre los derechos de acceso a la información pública y la protección de datos en las jornadas sobre transparencia celebradas en México D.F., en reuniones con Institutos de acceso a la información pública de México, en visitas institucionales a la AEPD y mediante la celebración de convenios con algunas de los citados institutos.

7. COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS DE PROTECCIÓN DE DATOS

La cooperación entre las Agencias de Protección de Datos es la base para garantizar la igualdad en la protección de la información personal de los ciudadanos, cualquiera que sea el lugar en que se traten sus datos.

El intercambio de información entre los Registros de ficheros de cada Agencia es fluido a través de los protocolos establecidos que incorporan las novedades del Reglamento de desarrollo de la LOPD.

En el ámbito de la inspección, las Agencias han compartido la preocupación sobre el ejercicio de derechos ante los responsables de servicios de buscador en Internet y ante los responsables de las ediciones electrónicas de diarios y boletines oficiales, ante la creciente casuística planteada. Es destacable también el intercambio de criterios sobre la vulneración de las medidas de seguridad y del deber de secreto en los casos de documentación encontrada en la vía pública, cuando están implicadas varias administraciones.

La colaboración entre las Agencias en 2009 ha tenido como principal hito la celebración en Madrid de la 31ª Conferencia Internacional de Protección de Datos y de la Privacidad.

Las Agencias Autonómicas han participado activamente con la AEPD en la elaboración de la "Propuesta Conjunta para la redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de datos de carácter Personar" presentada en la sesión cerrada de la Conferencia.

Asimismo colaboraron en la celebración de las reuniones preparatorias de los grupos de expertos y de trabajo de la elaboración y debate de la Propuesta celebradas en Barcelona y Bilbao, organizadas conjuntamente con la Agencia de Protección de Datos de Cataluña y la Agencia Vasca de Protección de Datos, respectivamente.

Durante la celebración de la 31ª Conferencia Internacional las Agencias Autonómicas aportaron su presencia institucional y sus directores intervinieron como ponentes en diversas sesiones de trabajo y manifestaron su apoyo a la Propuesta de Estándares Internacionales en la sesión cerrada en la que fueron adoptados.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RECOMENDACIONES

RECOMENDACIONES

A. RECOMENDACIONES NORMATIVAS

- Modificar la normativa reguladora del DNI-e para que los menores puedan autenticarse electrónicamente aunque no firmar electrónicamente.

B. RECOMENDACIONES EJECUTIVAS

- Extremar las precauciones en el ejercicio de las labores de recobro de morosos para la plena salvaguardia del secreto profesional sobre los datos de los presuntos deudores que evite comportamientos impropios de comunicación de la deuda a compañeros de trabajo, vecinos u otros allegados mediante contacto telefónico, envío a faxes u otros métodos.

- Potenciación por los Colegios Profesionales de mecanismos que permitan el depósito de datos de los afectados en caso de fallecimiento o desaparición de los responsables de fichero correspondientes a su ámbito profesional.

- La inclusión en los planes de estudio de primaria y secundaria de formación sobre protección de datos, privacidad e Internet, así como la puesta a disposición de los alumnos por parte de las Administraciones Públicas y los centros educativos de herramientas informáticas que eviten el acceso de los menores de 14 años a servicios de Internet para los que deban contar con el consentimiento de sus padres o representantes legales.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

LA AGENCIA EN CIFRAS

1. INSPECCIÓN

ACTUACIONES PREVIAS Y TUTELAS DE DERECHOS INICIADAS

TIPO	2007	2008	2009	% VAR. 2008/2009
Tutela de los derechos de acceso, rectificación, cancelación y oposición	896	1.687	**1.881**	+11,50
Actuaciones previas de inspección* (iniciadas a partir de denuncia o a iniciativa del Director)	1.624	2.362	**4.136**	+75,11
TOTAL	**2.520**	**4.049**	**6.017**	**+48,60**

* Las cifras incluyen procedimientos AT (admisión a trámite, solicitudes de mejora de la solicitud no subsanada), AR (acuerdo de no inicio de PS) y EI (actuaciones de inspección incoadas).

RESOLUCIONES

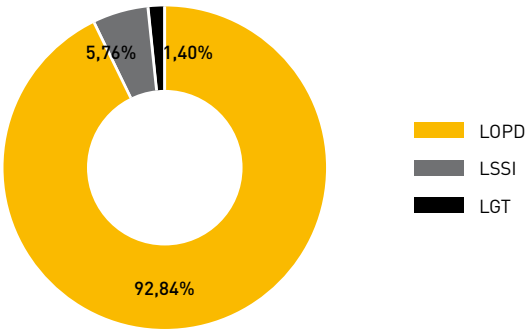
PROCEDIMIENTOS DE LA INSPECCIÓN DE DATOS	2007	2008	2009	% VAR. 2008/2009
Reclamaciones de tutela de los derechos de acceso, rectificación, cancelación y oposición (capitulo II)	849	1.229	**1.947**	+58,42
Procedimientos relativos al ejercicio de la potestad sancionadora (capítulo III)	1.246	2.419	**3.905**	+61,43
Archivo de actuaciones previas	781	1.710	**3.107**	+81,70
Procedimientos sancionadores resueltos	399	630	**709**	+12,54
Resolución sancionadora	342	535	**621**	+16,07
Resolución de archivo	57	95	**88**	-7,37
Procedimientos de infracción LOPD de las AAPP	66	79	**89**	+12,66
Declaración de infracción	49	59	**71**	+20,34
Declaración de no infracción	17	20	**18**	-10
TOTAL RESOLUCIONES	**2.095**	**3.648**	**5.852**	**+60,42**

SANCIONES IMPUESTAS

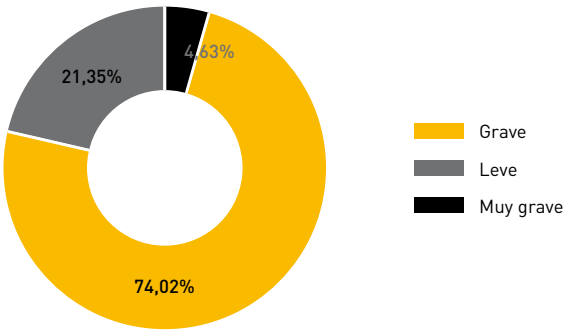
	2007	2008	2009	% VAR. 2008/2009
TOTAL	**17.584.198,42 €**	**22.013.632,57 €**	**24.872.979,72 €**	+12,99

La tabla recoge el total de sanciones declaradas.

SANCIONES IMPUESTAS SEGÚN LEY INFRINGIDA 2009



SANCIONES IMPUESTAS SEGÚN LA GRAVEDAD 2009



ACTUACIONES PREVIAS INICIADAS POR SECTORES

ACTIVIDAD	2008	2009	% relativo
Telecomunicaciones	454	**908**	21,95
Entidades financieras	382	**768**	18,57
Videovigilancia	365	**721**	17,43
Administración pública	122	**218**	5,27
Comunicaciones electrónicas comerciales – *spam* (LSSI)	147	**180**	4,35
Profesionales, comunidades de propietarios, administración de fincas	87	**160**	3,87
Servicios de Internet	104	**156**	3,77
Comercio, transporte y hostelería	117	**137**	3,31
Sanidad	75	**123**	2,97
Recursos humanos, asuntos laborales, mutuas	110	**120**	2,90
Asociaciones, federaciones, colegios profesionales, ONG's, fundaciones, clubes	55	**119**	2,88
Suministro y comercialización de gas, electricidad y agua	40	**53**	1,28
Publicidad y prospección comercial (excepto *spam*)	40	**52**	1,26
Medios de comunicación	23	**51**	1,23
Seguros	27	**47**	1,14
Enseñanza	22	**34**	0,82
Fuerzas y cuerpos de seguridad	40	**32**	0,77
Envío de comunicaciones comerciales por fax (LGT)	38	**25**	0,60
Sindicatos	30	**24**	0,58
Partidos políticos	15	**15**	0,36
Seguridad privada	5	**10**	0,24
Procedimientos judiciales	-	**3**	0,07
Otros	67	**180**	4,35
TOTAL	**2.362**	**4.136**	**100**

PROCEDIMIENTOS SANCIONADORES RESUELTOS POR SECTOR DE ACTIVIDAD

ACTIVIDAD	2007	2008	2009	% relativo	% VAR. 2008/2009
Telecomunicaciones	112	203	**182**	25,67	-10,34
Videovigilancia	6	44	**145**	20,45	+229,55
Entidades financieras	80	127	**100**	14,10	-21,26
Comunicaciones electrónicas comerciales – *spam* (LSSI)	37	46	**46**	6,49	0
Publicidad y prospección comercial (excepto *spam*)	29	26	**28**	3,95	+7,69
Asociaciones, federaciones, colegios profesionales, ONG's, fundaciones, clubes	11	11	**24**	3,39	+118,18
Comercio, transporte, hostelería	19	39	**23**	3,24	-41,03
Suministro y comercialización de gas, electricidad y agua	22	13	**21**	2,96	+61,54
Profesionales, comunidades de propietarios, administración de fincas	10	13	**19**	2,68	+46,15
Recursos humanos, asuntos laborales, mutuas	2	9	**18**	2,54	+100
Servicios de Internet	6	13	**17**	2,40	+30,77
Comunicaciones comerciales por fax (LGT)	2	9	**12**	1,69	+33,33
Seguros	4	6	**10**	1,41	+66,67
Sindicatos	5	8	**9**	1,27	+12,50
Sanidad	4	10	**8**	1,13	-20
Partidos políticos	2	6	**7**	0,99	+16,67
Administración Pública (entidades de derecho privado)	0	3	**5**	0,71	+66,67
Enseñanza	5	1	**5**	0,71	+400
Informaciones publicadas en medios de comunicación	1	2	**2**	0,28	0
Otros	42	41	**28**	3,95	-31,71
TOTAL	**399**	**630**	**709**	**100**	**+12,54**

Se incluyen procedimientos que finalizan con archivo o sanción.

RESOLUCIONES SANCIONADORAS POR SECTOR DE ACTIVIDAD

ACTIVIDAD	2008	2009	% relativo
Telecomunicaciones	190	**170**	27,38
Videovigilancia	27	**117**	18,84
Entidades financieras	111	**89**	14,33
Comunicaciones electrónicas comerciales - *spam* (LSSI)	39	**39**	6,28
Publicidad (excepto *spam*)	22	**24**	3,86
Comercio, transporte y hostelería	31	**22**	3,54
Suministro y comercialización de gas, electricidad y agua	11	**21**	3,38
Asociaciones, federaciones, colegios profesionales, ONG's, fundaciones, clubes	10	**20**	3,22
Recursos humanos, asuntos laborales, mutuas	5	**17**	2,74
Servicios de Internet	10	**16**	2,58
Profesionales, comunidades de propietarios, administración de fincas	10	**15**	2,42
Envío de comunicaciones comerciales por fax (LGT)	7	**11**	1,77
Seguros	5	**8**	1,29
Sanidad	9	**6**	0,97
Administración pública (entidades de derecho privado)	2	**5**	0,81
Enseñanza	1	**5**	0,81
Partidos políticos	6	**5**	0,81
Sindicatos	5	**4**	0,64
Medios de comunicación	3	**2**	0,32
Otros	31	**25**	4,03
TOTAL	**535**	**621**	**100**

Resoluciones que finalizan con imposición de sanción.

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS

TIPO ADMINISTRACIÓN	2007	2008	2009	% relativo	% VAR. 2008/2009
Autonómica	16	21	**29**	32,58	+38,10
Local	28	32	**22**	24,72	-31,25
Otras Entidades de Derecho Público	-	5	**21**	23,60	+320
Estatal	22	21	**17**	19,10	-19,05
TOTAL	**66**	**79**	**89**	**100**	**+12,66**

Se incluyen procedimientos que finalizan con archivo o declaración de infracción de las AAPP.

INFRACCIONES DE LAS ADMINISTRACIONES PÚBLICAS

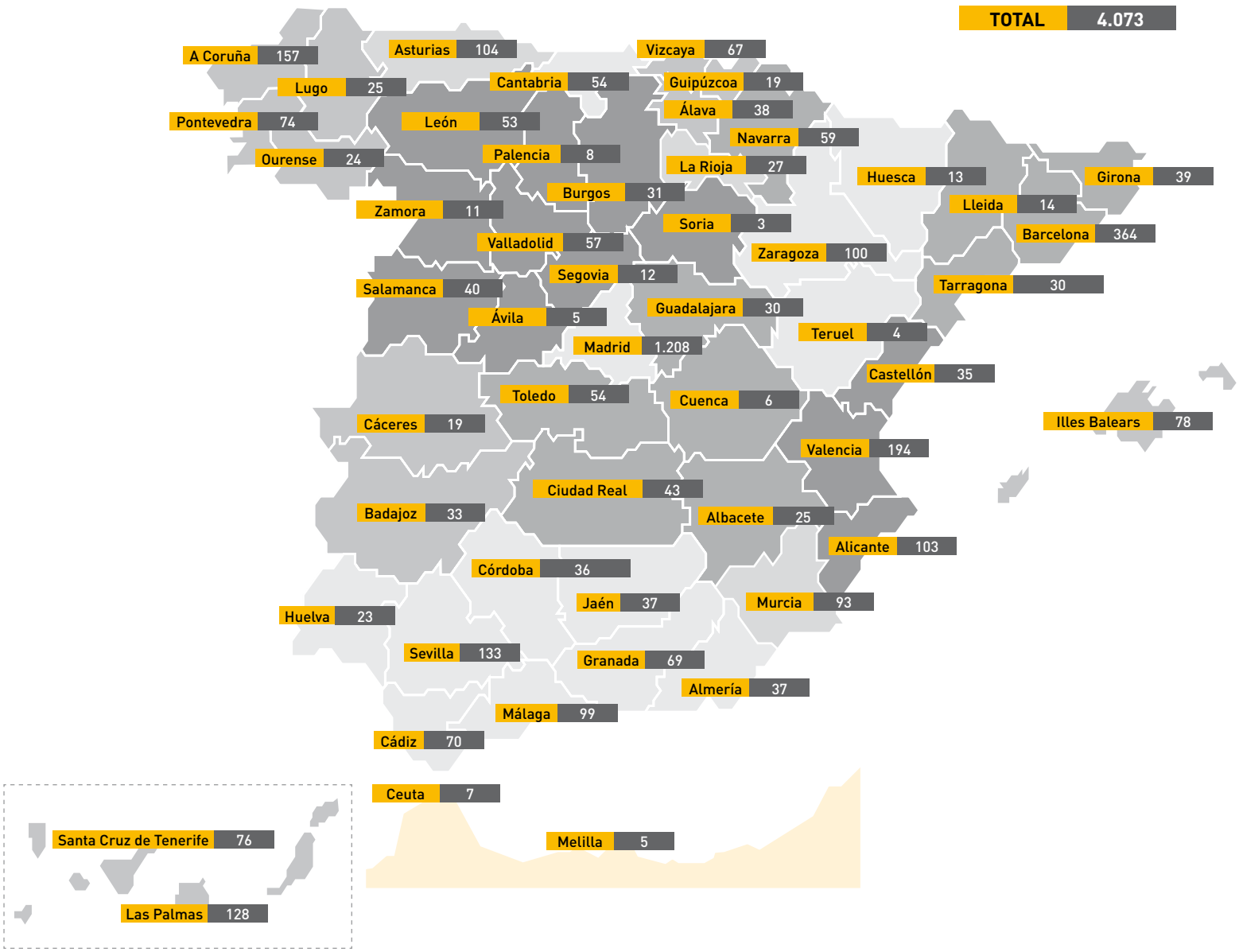
TIPO ADMINISTRACIÓN	2009	% VAR. 2008/2009
Local	**18**	25,35
Autonómica	**24**	33,80
Estatal	**13**	18,31
Otras Entidades de Derecho Público	**16**	22,54
TOTAL	**71**	**100**

Resoluciones que finalizan con declaración de infracción de las AAPP.

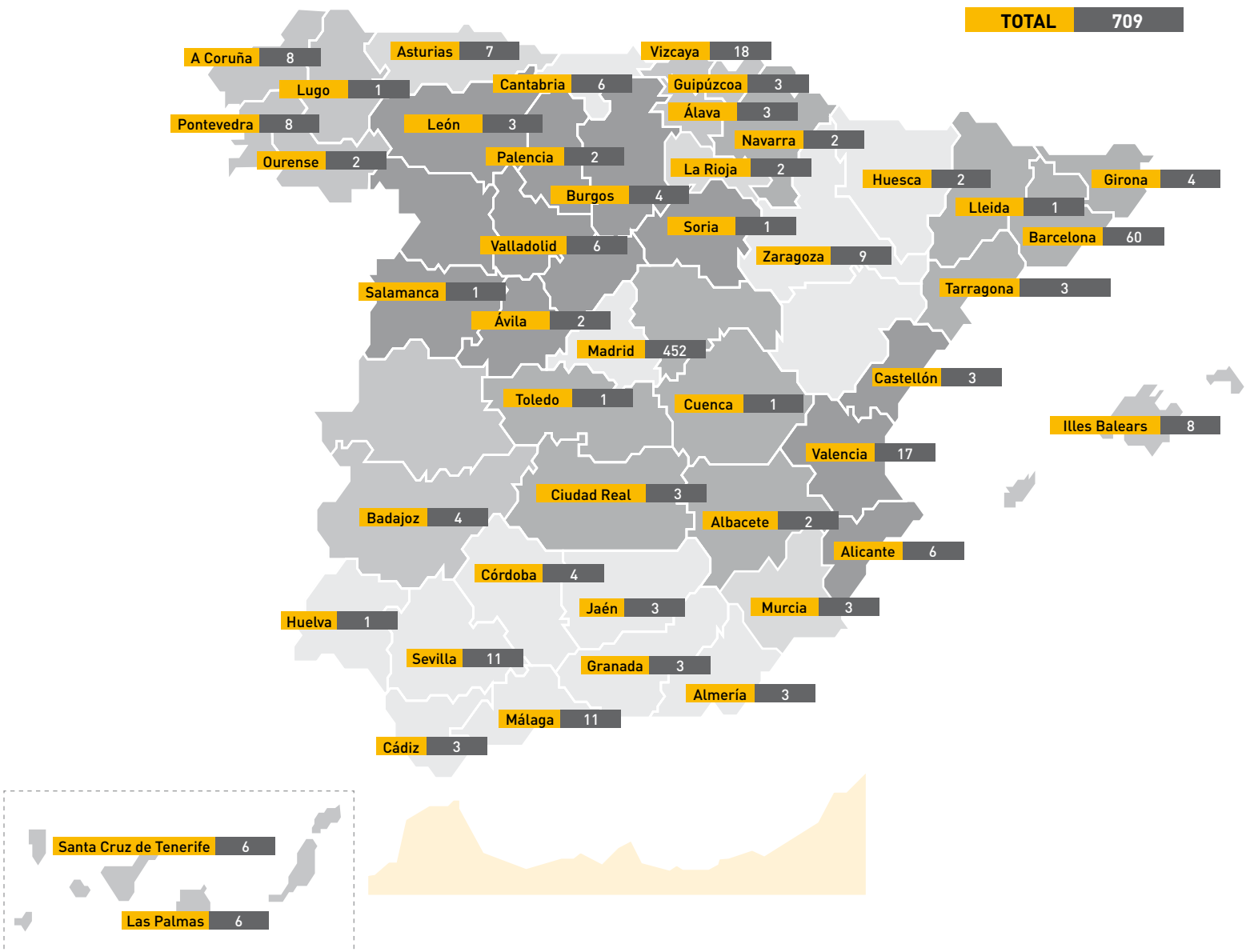
TUTELAS DE DERECHOS RESUELTAS

DERECHOS TUTELADOS	RESOLUCIÓN					
	Estimatoria	Estimatoria Formal-Parcial	Desestimat.	Desistim.	Archiv. Inadmitida	Total
Cancelación	204	51	551	3	557	1.366
Acceso	92	136	90	14	58	390
Rectificación	-	-	18	-	4	22
Oposición	58	27	40	-	2	127
Varios derechos	1	21	6	-	14	42
TOTAL	**355**	**235**	**705**	**17**	**635**	**1.947**

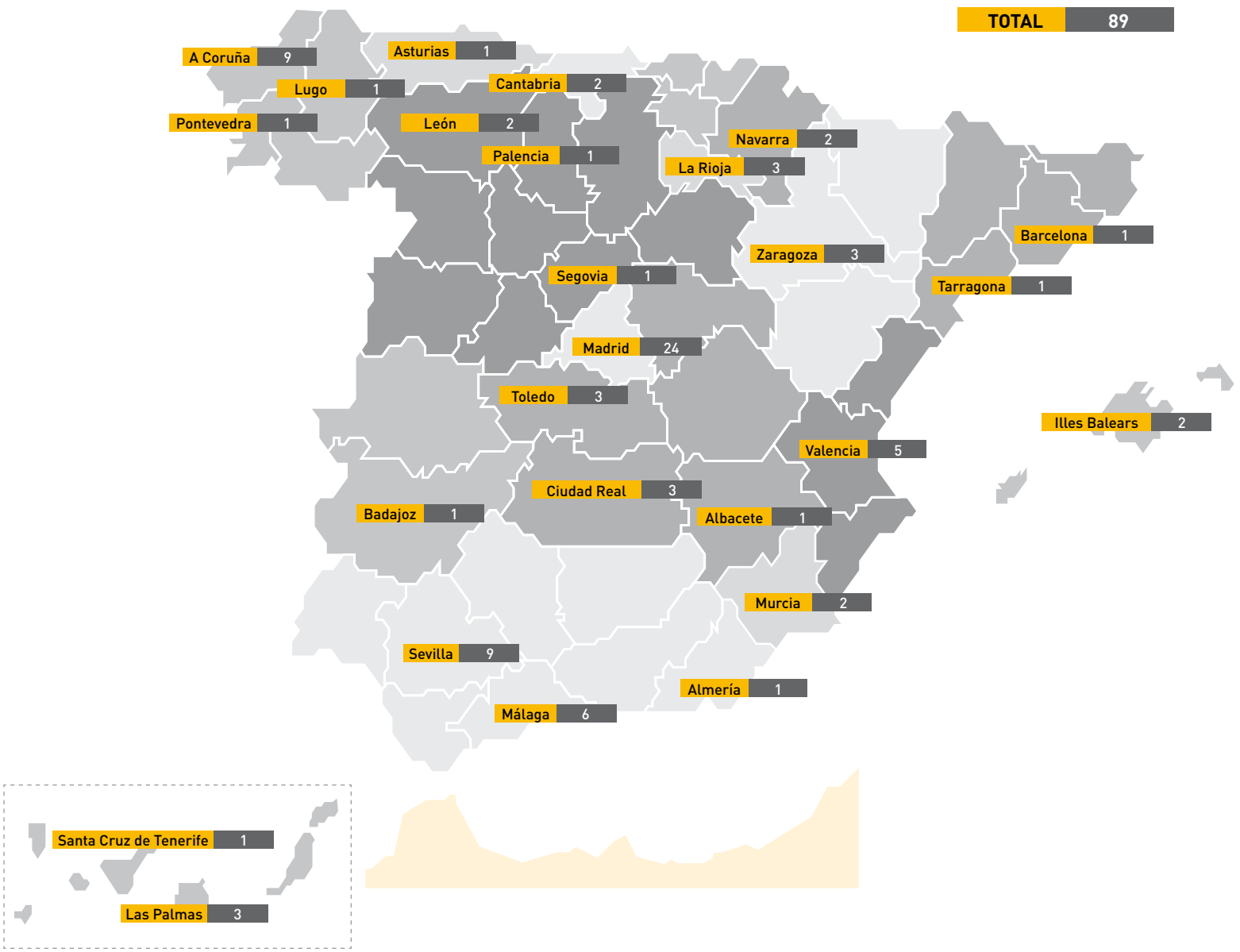
DISTRIBUCIÓN GEOGRÁFICA DE LAS DENUNCIAS (PROVINCIA DEL DENUNCIANTE)



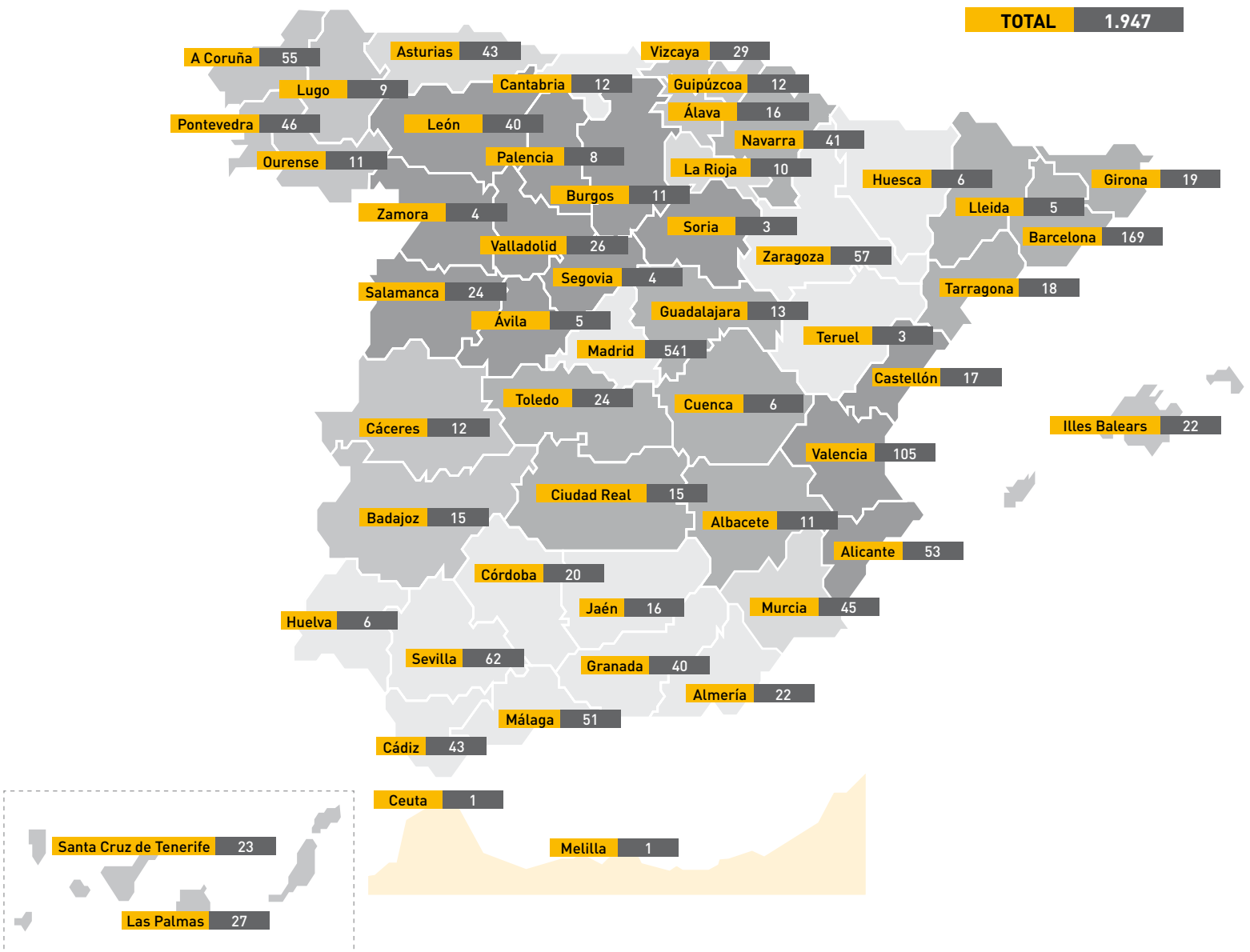
DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS SANCIONADORES



DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS AAPP



DISTRIBUCIÓN GEOGRÁFICA DE PROCEDIMIENTOS INICIADOS DE TUTELA DE DERECHOS (PROVINCIA DEL RECLAMANTE)



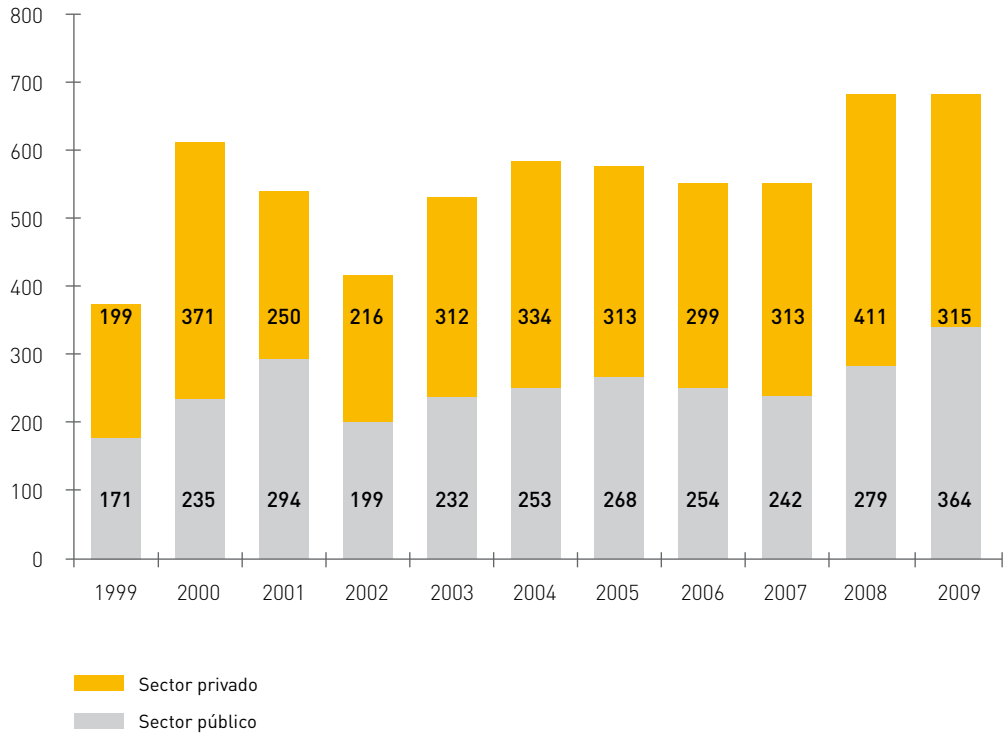
2. GABINETE JURÍDICO

CONSULTAS

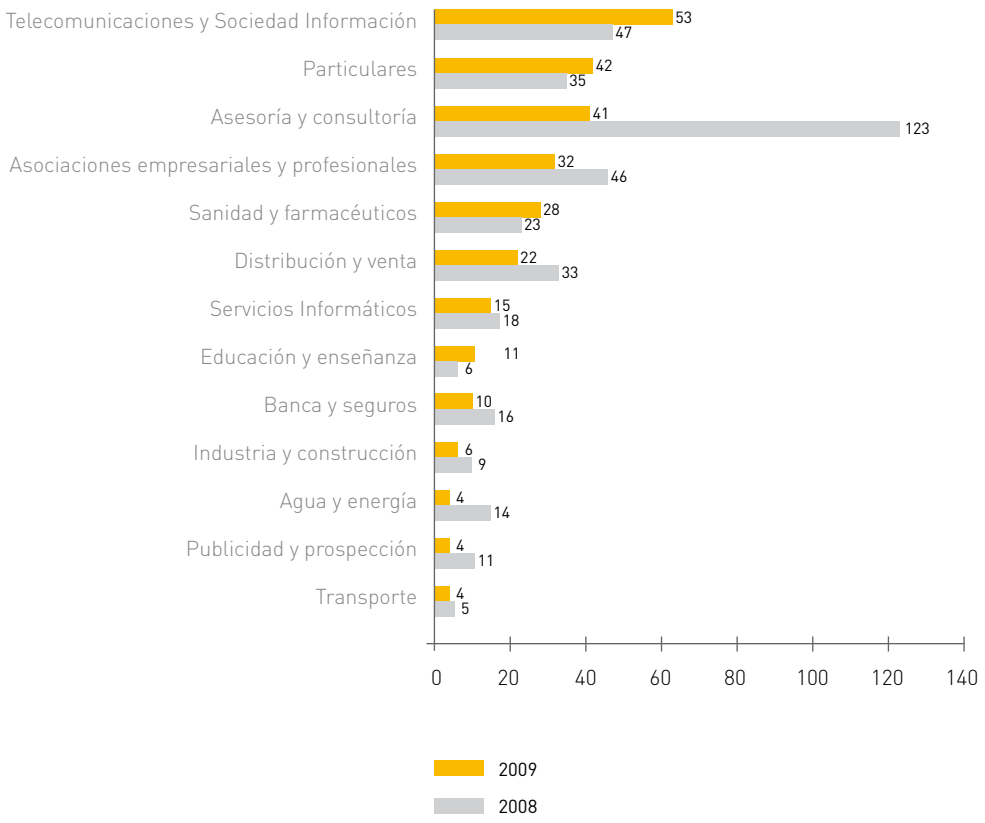
ADMINISTRACIONES PÚBLICAS	364
Administración General del Estado	174
Comunidades Autónomas	39
Entidades Locales	83
Otros Organismos Públicos	68

CONSULTAS PRIVADAS	315
Empresas	224
Particulares	40
Asociaciones/Fundaciones	35
Sindicatos	14
Otros	2

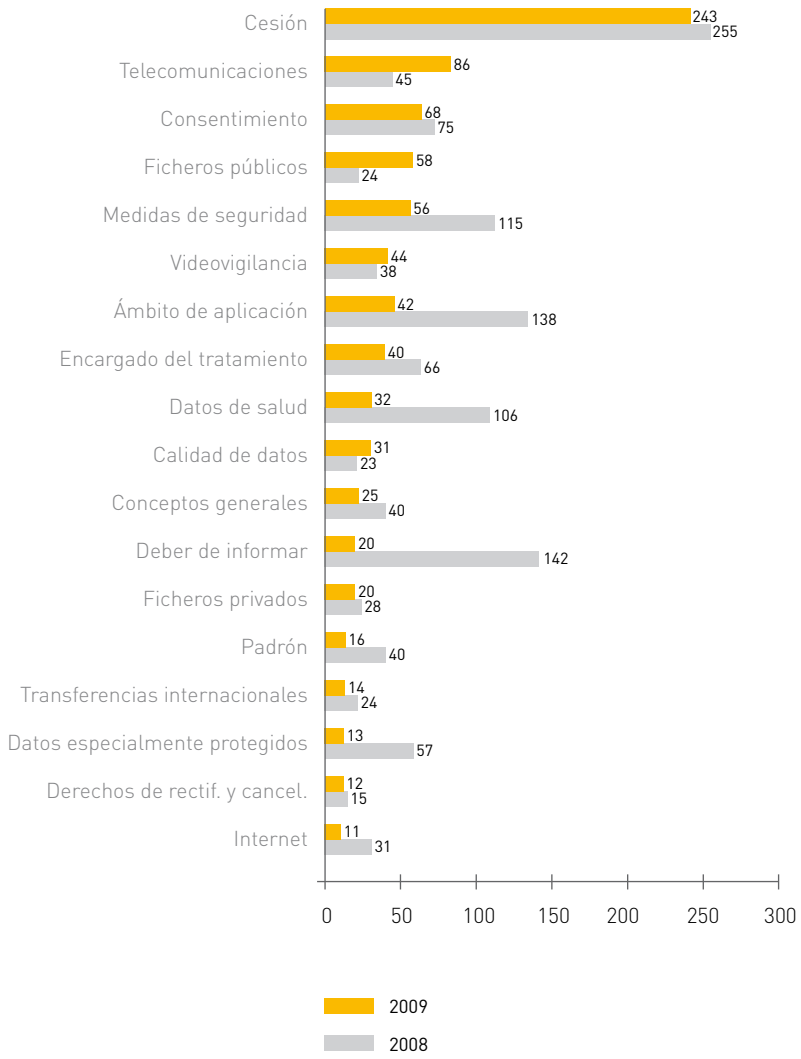
EVOLUCIÓN DE LAS CONSULTAS (1999-2009)



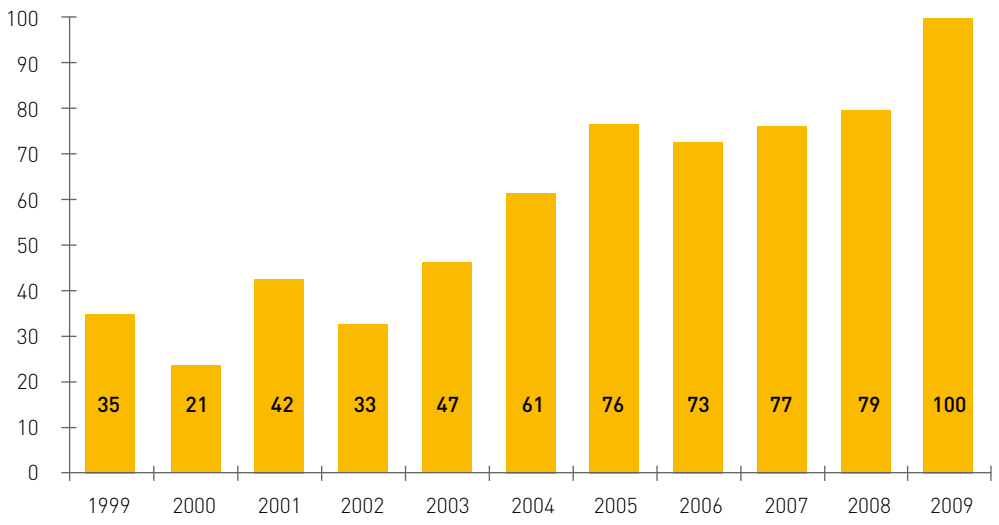
EVOLUCIÓN POR SECTORES (2008-2009)



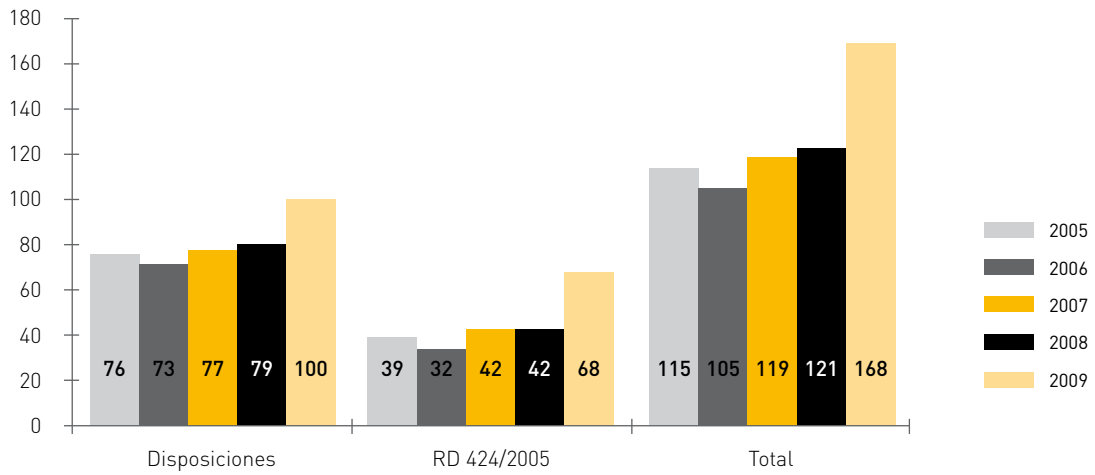
EVOLUCIÓN POR MATERIAS (2008-2009)



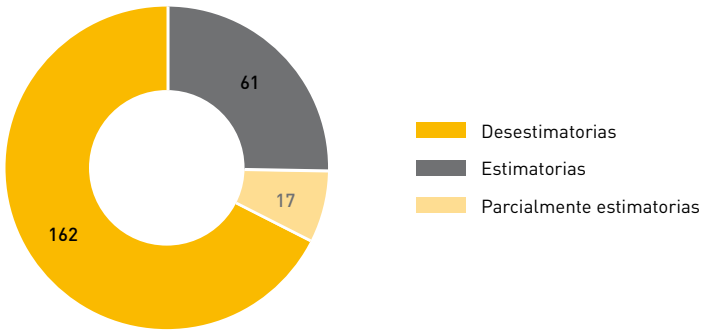
EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (1999-2009)



INFORMES PRECEPTIVOS (2005-2009)

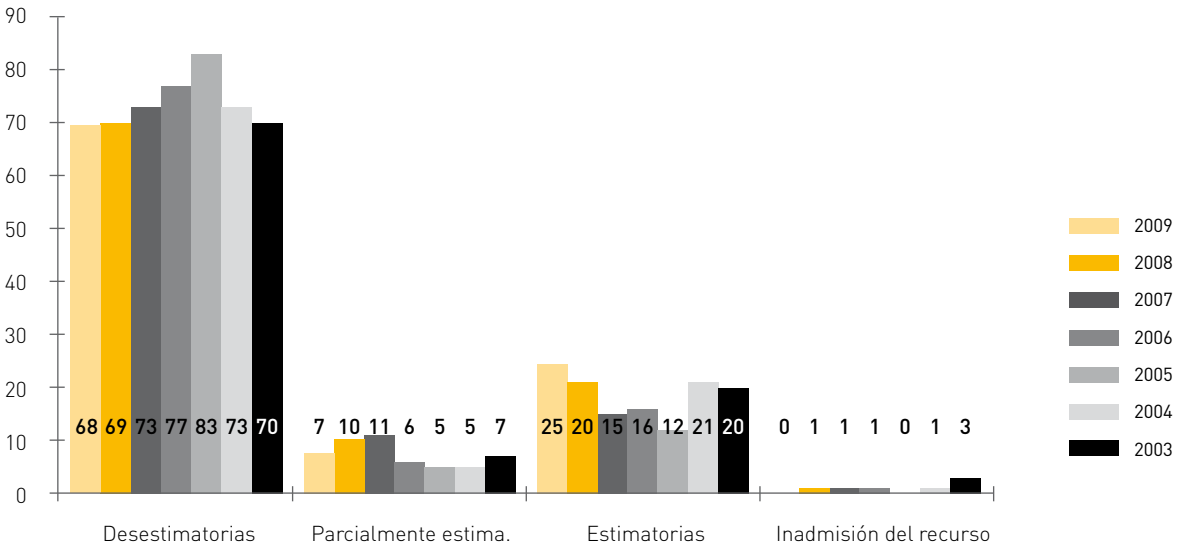


SENTENCIAS DE LA AUDIENCIA NACIONAL



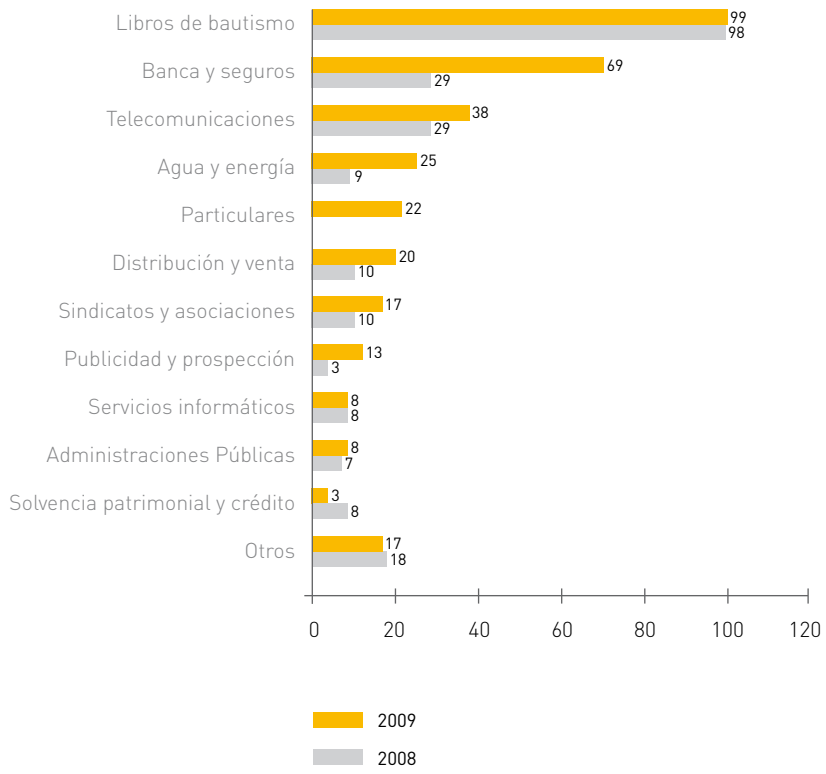
El gráfico exceptúa las cifras relativas a las sentencias dictadas por la AN referidas al ejercicio de cancelación en libros de bautismo.

COMPARATIVA SENTENCIAS DE LA AUDIENCIA NACIONAL

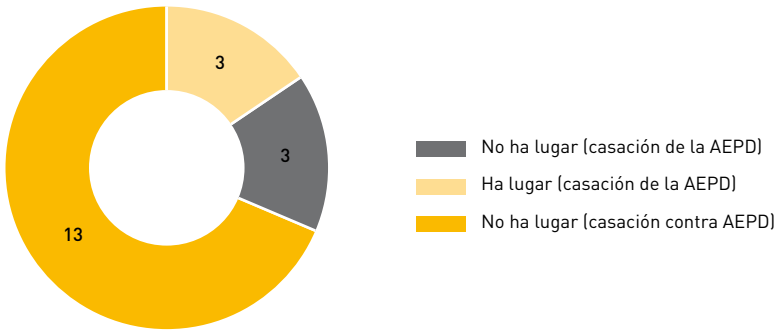


El gráfico exceptúa las cifras relativas a las sentencias dictadas en 2008 y 2009 por la AN referidas al ejercicio de cancelación en libros de bautismo.

COMPARATIVA SENTENCIAS AUDIENCIA NACIONAL POR SECTORES (2008-2009)



SENTENCIAS DEL TRIBUNAL SUPREMO



El gráfico exceptúa las cifras relativas a las sentencias dictadas por el TS referidas al ejercicio de cancelación en libros de bautismo.

3. ATENCIÓN AL CIUDADANO

CONSULTAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención telefónica	Atención presencial	Atención por escrito	Total	Porcentaje de incremento
Año 2005	26.654	2.938	5.420	35.512	1,53%
Año 2006	27.486	2.030	6.323	35.839	0,9%
Año 2007	33.908	4.185	9.648	47.741	30,09%
Año 2008	58.143	4.785	9.722	72.650	52,17%
Año 2009	**77.359**	**4.277**	**15.587***	**97.223**	**33,82%**

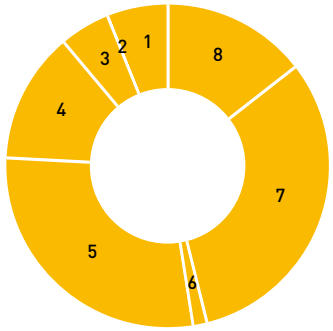
* En el año 2009, 13.776 consultas escritas se contestaron a través del buzón electrónico ciudadano@agpd.es.

COMPARACION DE ACCESOS A LA PÁGINA WEB CON EL AÑO 2008

AÑO	2008	2009
Acceso a web	2.277.065	**2.998.276**
Promedio diario	6.238,5	**8.214,4**

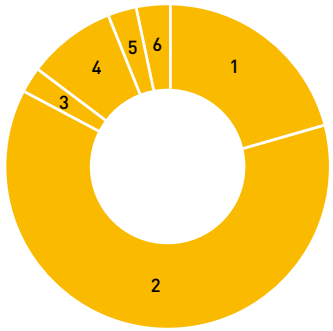
ANÁLISIS DE LAS CONSULTAS POR TEMAS 2009

TEMAS	Porcentaje
1. Información	5,94%
2. Inscripción ficheros	0,16%
3. Principios LOPD	4,75%
4. Otros	13,24%
5. Ambito de aplicación	28,27%
6. Cesión	1,4%
7. Derechos	31,7%
8. Ficheros concretos	14,43%



CONSULTAS SOBRE DERECHOS 2009

TEMAS	Porcentaje
1. Acceso	20,62%
2. Cancelación	62,39%
3. Rectificación	2,42%
4. Oposición	8,66%
5. Información	2,77%
6. Otras consultas sobre derechos	3,11%



4. REGISTRO GENERAL DE PROTECCIÓN DE DATOS

DERECHO DE CONSULTA AL REGISTRO

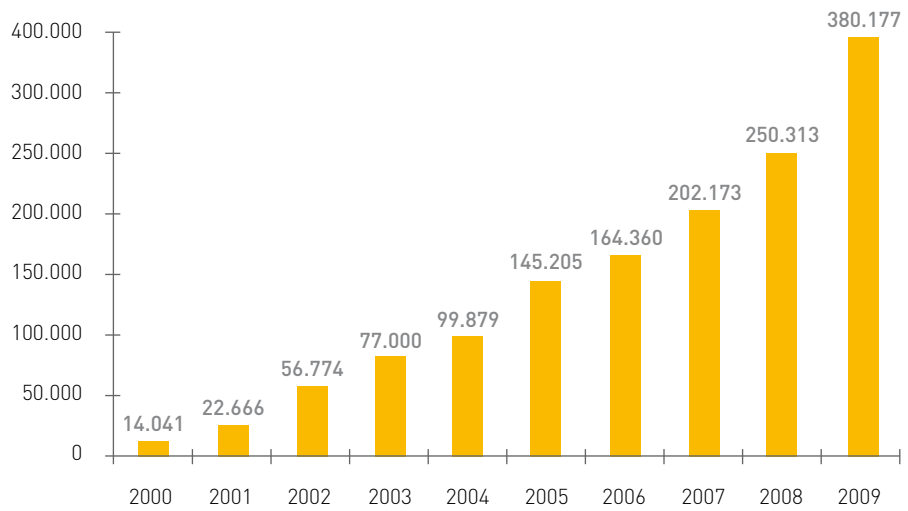
TITULARIDAD	2008	2009
Privada	818.248	**1.356.216**
Pública	691.144	**1.070.173**
TOTAL	**1.509.392**	**2.426.389**

EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

Ficheros inscritos

TITULARIDAD	2003	2004	2005	2006	2007	2008	2009
Privada	361.675	457.490	598.916	758.955	955.713	1.182.496	**1.552.060**
Pública	43.974	48.038	51.817	56.138	61.553	85.083	**95.696**
TOTAL	**405.649**	**505.528**	**650.733**	**815.093**	**1.017.266**	**1.267.579**	**1.647.756**

Incremento anual total

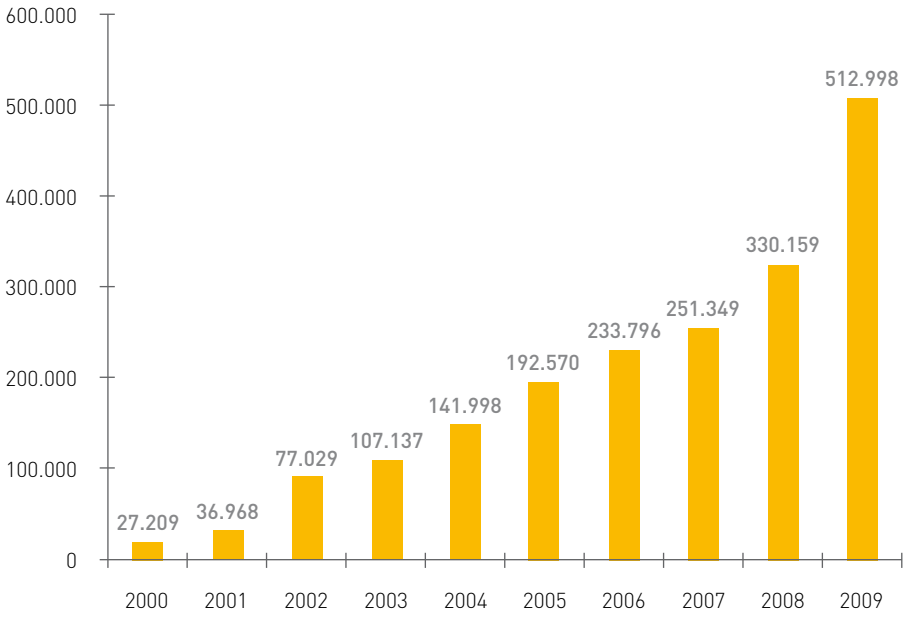


EVOLUCIÓN DE LA INSCRIPCIÓN EN EL RGPD

Datos relacionados con la inscripción

	2008	2009	% VAR. 2008/2009	Media diaria en 2008	Media diaria en 2009
Operaciones de inscripción	330.159	**512.998**	+55	1.376	**2.137**
Total de ficheros inscritos	1.267.579	**1.647.756**	+30	1.043	**1.584**

Incremento anual de las operaciones de inscripción



INSCRIPCIÓN DE TITULARIDAD PRIVADA

Distribución de ficheros

	Responsables		Ficheros	
	2009	Total	2009	Total
Comunidad Autónoma de Andalucía	25.709	**70.879**	66.767	**200.930**
Almería	**3.096**	7.216	**8.290**	21.300
Cádiz	**2.378**	7.516	**6.231**	21.449
Córdoba	**2.487**	7.001	**6.147**	19.475
Granada	**4.516**	11.390	**12.409**	36.571
Huelva	**953**	2.567	**3.109**	8.646
Jaén	**2.547**	5.969	**7.144**	19.282
Málaga	**5.525**	16.763	**12.869**	37.897
Sevilla	**4.306**	12.872	**10.568**	36.310
Comunidad Autónoma de Aragón	4.808	**24.547**	11.621	**53.772**
Huesca	**922**	4.826	**2.456**	10.318
Teruel	**590**	1.784	**1.507**	4.166
Zaragoza	**3.303**	17.976	**7.658**	39.288
Comunidad Autónoma del Principado de Asturias	6.104	**19.607**	17.392	**61.483**
Comunidad Autónoma de Canarias	4.933	**17.822**	14.478	**62.700**
Las Palmas	**2.238**	7.878	**6.654**	29.303
Santa Cruz de Tenerife	**2.706**	9.994	**7.824**	33.397
Comunidad Autónoma de Cantabria	1.698	**6.232**	3.769	**13.363**
Comunidad Autónoma de Castilla y León	7.912	**26.404**	22.682	**66.802**
Ávila	**508**	1.785	**1.101**	3.532
Burgos	**1.077**	5.134	**2.889**	11.982
León	**1.576**	5.305	**4.086**	13.355
Palencia	**799**	2.105	**2.225**	5.215
Salamanca	**821**	2.744	**2.263**	6.783
Segovia	**729**	1.675	**1.897**	4.091
Soria	**275**	872	**955**	2.387
Valladolid	**1.306**	5.124	**3.749**	13.489
Zamora	**826**	1.726	**3.517**	5.968

	Responsables		Ficheros	
	2009	Total	2009	Total
Comunidad Autónoma de Castilla-La Mancha	**6.800**	**17.227**	**19.777**	**52.141**
Albacete	**2.571**	5.737	**8.395**	18.137
Ciudad Real	**1.036**	3.211	**2.916**	10.864
Cuenca	**591**	1.935	**1.387**	4.642
Guadalajara	**460**	1.636	**1.184**	4.370
Toledo	**2.148**	4.750	**5.895**	14.128
Comunidad Autónoma de Cataluña	**23.436**	**143.657**	**59.931**	**331.897**
Barcelona	**16.506**	107.386	**40.783**	246.781
Girona	**3.268**	17.295	**8.898**	39.448
Lleida	**1.073**	7.340	**3.083**	17.426
Tarragona	**2.599**	11.876	**7.167**	28.242
Comunidad de Madrid	**26.710**	**101.852**	**54.757**	**238.660**
Comunidad Valenciana	**16.865**	**69.876**	**39.837**	**158.515**
Alicante	**6.307**	23.330	**13.782**	50.352
Castellón de la Plana	**1.857**	8.401	**4.738**	20.930
Valencia	**8.710**	38.222	**21.317**	87.233
Comunidad Autónoma de Extremadura	**2.563**	**9.793**	**6.623**	**25.671**
Badajoz	**1.660**	6.586	**4.044**	4.044
Cáceres	**906**	3.221	**2.579**	2.579
Comunidad Autónoma de Galicia	**13.207**	**40.295**	**31.356**	**113.549**
A Coruña	**6.684**	17.743	**14.795**	46.918
Lugo	**1.647**	5.925	**3.986**	16.149
Ourense	**1.290**	3.498	**3.345**	10.302
Pontevedra	**3.600**	13.239	**9.230**	40.179
Comunidad Autónoma de las Illes Balears	**3.919**	**11.667**	**11.645**	**38.002**
Comunidad Foral de Navarra	**1.755**	**7.124**	**4.512**	**19.012**
Comunidad Autónoma del País Vasco	**6.310**	**23.854**	**13.934**	**60.351**
Álava	**539**	2.999	**1.346**	8.097
Guipúzcoa	**1.514**	7.556	**3.274**	18.767
Vizcaya	**4.260**	13.345	**9.314**	33.487
Comunidad Autónoma de la Rioja	**1.061**	**6.190**	**2.487**	**15.335**
Comunidad Autónoma de la Región de Murcia	**5.101**	**16.277**	**11.754**	**38.892**
Ciudad Autónoma de Ceuta	**71**	**279**	**178**	**737**
Ciudad Autónoma de Melilla	**49**	**200**	**121**	**477**

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2009	Total
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**14.282**	53.080
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**52.944**	237.757
Datos de carácter identificativo	**393.626**	1.552.060
Datos de características personales	**165.135**	654.735
Datos de circunstancias sociales	**99.139**	364.140
Datos académicos y profesionales	**102.881**	351.035
Detalles de empleo y carrera administrativa	**120.680**	502.947
Datos de información comercial	**118.645**	393.740
Datos económico-financieros	**209.282**	895.113
Datos de transacciones	**172.750**	585.756
Otros tipos de datos	**25.533**	52.291

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2009	Total	% sobre total
Gestión de clientes, contable, fiscal y administrativa	**223.103**	1.044.968	21,35 %
Recursos humanos	**91.578**	350.120	26,16 %
Gestión de nóminas	**72.049**	258.381	27,88 %
Prevención riesgos laborales	**35.597**	104.327	34,12 %
Publicidad y prospección comercial	**23.822**	125.081	19,05 %
Videovigilancia	**21.202**	33.817	62,70 %
Gestión y control sanitario	**16.676**	83.415	19,99 %
Historial clínico	**10.233**	55.847	18,32 %
Cumplimiento/incumplimiento de obligaciones dinerarias	**6.792**	34.654	19,60 %
Comercio electrónico	**6.758**	16.957	39,85 %
Seguridad y control acceso a edificios	**6.466**	19.880	32,53 %
Educación	**5.201**	24.121	21,56 %
Fines históricos, científicos o estadísticos	**5.072**	73.761	6,88 %
Actividades asociativas diversas	**5.048**	32.811	15,39 %
Análisis de perfiles	**4.717**	15.336	30,76 %
Servicios económico-financieros y seguros	**4.006**	58.517	6,85 %
Prestación de servicios de telecomunicaciones	**2.054**	8.083	25,41 %
Asistencia social	**2.013**	6.897	29,19 %
Seguridad privada	**1.905**	8.171	23,31 %
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro	**1.896**	7.862	24,12 %
Guías/repertorios de servicios de telecomunicaciones	**915**	2.989	30,61 %
Investigación epidemiológica y actividades análogas	**820**	7.181	11,42 %
Prestación de servicios de solvencia patrimonial y crédito	**607**	6.110	9,93 %
Prestación de servicios de certificación	**352**	1.577	22,32 %
Otras finalidades	**61.946**	217.657	28,46 %

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2009	Total	% sobre total
Comunidades de propietarios	**52.297**	195.652	26,73%
Comercio	**44.303**	170.528	25,98%
Sanidad	**30.279**	131.145	23,09%
Contabilidad, auditoría y asesoría fiscal	**18.698**	96.833	19,31%
Construcción	**17.121**	64.758	26,44%
Turismo y hostelería	**16.852**	57.841	29,14%
Actividades jurídicas, notarios y registradores	**11.176**	47.253	23,65%
Industria química y farmacéutica	**10.902**	46.471	23,46%
Transporte	**10.459**	33.714	31,02%
Educación	**10.450**	39.916	26,18%
Actividades inmobiliarias	**8.040**	66.384	12,11%
Asociaciones y clubes	**7.485**	40.901	18,30%
Servicios informáticos	**5.487**	28.699	19,12%
Actividades relacionadas con los productos alimenticios, bebidas y tabacos	**5.273**	22.532	23,40%
Agricultura, ganadería, explotación forestal, caza y pesca	**4.892**	20.015	24,44%
Maquinaria y medios de transporte	**4.350**	29.121	14,94%
Actividades de servicios sociales	**4.271**	15.744	27,13%
Actividades diversas de servicios personales	**4.141**	15.773	26,25%
Seguros privados	**3.064**	22.264	13,76%
Producción de bienes de consumo	**3.011**	16.272	18,50%
Sector energético	**2.696**	14.050	19,19%
Servicios de telecomunicaciones	**2.117**	8.075	26,22%
Comercio y servicios electrónicos	**2.044**	4.057	50,38%
Actividades políticas, sindicales y religiosas	**1.997**	4.669	42,77%
Actividades de organizaciones empresariales, profesionales y patronales	**1.546**	9.659	16,01%
Seguridad	**1.255**	5.094	24,64%
Publicidad directa	**1.202**	7.631	15,75%
Actividades relacionadas con los juegos de azar y apuestas	**759**	4.532	16,75%
Entidades bancarias y financieras	**648**	12.404	5,22%
Organización de ferias, exhibiciones, congresos y otras actividades relacionadas	**599**	2.006	29,86%
Investigación y desarrollo (I+D)	**538**	2.834	18,98%
Inspección Técnica de vehículos y otros análisis técnicos	**424**	1.403	30,22%
Selección de personal	**380**	3.527	10,77%
Actividades postales y de correo (operadores postales, empresas prestadoras de servicios postales, transportistas y empresas de actividades auxiliares y complementarias del transporte)	**260**	2.245	11,58%
Solvencia patrimonial y crédito	**98**	896	10,94%
Mutualidades colaboradoras de los organismos de la Seguridad Social	**50**	849	5,89%
Otras actividades	**104.463**	271.291	38,51%

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN	2009	Total
Administración General	**520**	4.363
Administración CC.AA.	**3.146**	17.218
Administración Local	**7.056**	50.615
Otras personas jurídico-públicas	**1.583**	23.500
TOTAL	**12.305**	**95.696**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	Ficheros
Presidencia del Gobierno	23
Ministerio de Asuntos Exteriores y de Cooperación	531
Ministerio de Justicia	41
Ministerio de Defensa	121
Ministerio de Economía y Hacienda	369
Ministerio del Interior	192
Ministerio de Fomento	368
Ministerio de Educación	116
Ministerio de Trabajo e Inmigración	1.195
Ministerio de la Presidencia	129
Ministerio de Política Territorial	164
Ministerio de Sanidad y Política Social	172
Ministerio de Medio Ambiente, y Medio Rural y Marino	332
Ministerio de Industria, Turismo y Comercio	246
Ministerio de Cultura	183
Ministerio de Vivienda	23
Ministerio de Igualdad	29
Ministerio de Ciencia e Innovación	129
TOTAL	**4.363**

DISTRIBUCIÓN DE FICHEROS DE COMUNIDADES AUTÓNOMAS

	2009	Ficheros
Comunidad Autónoma de Andalucía	**114**	1.846
Comunidad Autónoma de Aragón	**23**	308
Comunidad Autónoma del Principado de Asturias	**35**	296
Comunidad Autónoma de Canarias	**27**	429
Comunidad Autónoma de Cantabria	**61**	154
Comunidad Autónoma de Castilla y León	**37**	741
Comunidad Autónoma de Castilla-La Mancha	**207**	565
Comunidad Autónoma de Cataluña	**57**	796
Comunidad de Madrid	**2.137**	8.542
Comunidad Valenciana	**56**	622
Comunidad Autónoma de Extremadura	**8**	354
Comunidad Autónoma de Galicia	**145**	454
Comunidad Autónoma de las Illes Balears	**156**	382
Comunidad Foral de Navarra	**7**	142
Comunidad Autónoma del País Vasco	**49**	894
Comunidad Autónoma de La Rioja	**15**	272
Comunidad Autónoma de la Región de Murcia	**11**	329
Ciudad Autónoma de Ceuta	**-**	23
Ciudad Autónoma de Melilla	**1**	69
TOTAL	**3.146**	**17.218**

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

Ficheros de la administración local

	Entidades	Ficheros
Comunidad Autónoma de Andalucía	**729**	**7.102**
Almería	104	1.107
Cádiz	46	624
Córdoba	77	680
Granada	169	1.362
Huelva	85	1.155
Jaén	86	570
Málaga	58	589
Sevilla	104	1.015
Comunidad Autónoma de Aragón	**500**	**4.032**
Huesca	182	1.403
Teruel	49	204
Zaragoza	269	2.425
Comunidad Autónoma del Principado de Asturias	**69**	**780**
Comunidad Autónoma de Canarias	**92**	**1.072**
Las Palmas	39	425
Santa Cruz de Tenerife	53	647
Comunidad Autónoma de Cantabria	**52**	**508**
Comunidad Autónoma de Castilla y León	**595**	**3.081**
Ávila	41	407
Burgos	100	372
León	200	1.112
Palencia	22	154
Salamanca	83	357
Segovia	17	88
Soria	10	37
Valladolid	85	390
Zamora	37	164

	Entidades	Ficheros
Comunidad Autónoma de Castilla-La Mancha	**409**	**5.657**
Albacete	94	3.354
Ciudad Real	109	687
Cuenca	85	695
Guadalajara	16	105
Toledo	105	816
Comunidad Autónoma de Cataluña	**825**	**8.014**
Barcelona	399	4.197
Girona	168	1.826
Lleida	150	1.123
Tarragona	111	868
Comunidad de Madrid	**209**	**2.734**
Comunidad Valenciana	**442**	**5.150**
Alicante	144	1.726
Castellón de la Plana	94	746
Valencia	205	2.678
Comunidad Autónoma de Extremadura	**213**	**1.925**
Badajoz	162	1.586
Cáceres	51	339
Comunidad Autónoma de Galicia	**300**	**2.590**
A Coruña	95	839
Lugo	63	488
Ourense	77	690
Pontevedra	65	573
Comunidad Autónoma de las Illes Balears	**79**	**1.288**
Comunidad Foral de Navarra	**131**	**1.193**
Comunidad Autónoma del País Vasco	**265**	**4.340**
Álava	50	392
Guipúzcoa	99	1.738
Vizcaya	117	2.210
Comunidad Autónoma de la Rioja	**37**	**264**
Comunidad Autónoma de la Región de Murcia	**46**	**885**

DISTRIBUCIÓN DE FICHEROS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS

	Total
Cámaras Oficiales de Comercio e Industria	414
Notariado	7.435
Universidades	813
Colegios Profesionales	1.706
Otros	13.132
TOTAL	**23.500**

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2009	Total
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**908**	17.126
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**3.237**	26.140
Datos relativos a infracciones	**2.572**	18.762
Datos de carácter identificativo	**12.305**	95.696
Datos de características personales	**6.373**	52.370
Datos de circunstancias sociales	**3.742**	27.264
Datos académicos y profesionales	**4.805**	30.275
Detalles de empleo y carrera administrativa	**3.618**	33.962
Datos de información comercial	**1.582**	12.203
Datos económico-financieros	**5.401**	45.167
Datos de transacciones	**1.607**	19.662
Otros tipos de datos	**1.603**	14.827

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES	2009	Total
Datos especialmente protegidos	**908**	**17.126**
Ideología	475	8.630
Creencias	360	8.276
Religión	381	8.340
Afiliación Sindical	770	16.554
Otros datos especialmente protegidos	**3.237**	**26.140**
Origen Racial	1.437	10.239
Salud	3.219	26.040
Vida Sexual	479	8.906
Datos relativos a infracciones	**2.572**	**18.762**
Infracciones Penales	902	14.525
Infracciones Administrativas	2.499	18.253

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2009	Total	% sobre total
Procedimiento administrativo	**4.889**	30.511	16,02%
Fines científicos, históricos o estadísticos	**2.499**	18.007	13,88%
Función estadística pública	**2.196**	11.552	19,01%
Recursos humanos	**2.086**	18.615	11,21%
Educación y cultura	**1.765**	8.762	20,14%
Gestión contable, fiscal y administrativa	**1.230**	15.632	7,87%
Gestión de nómina	**668**	9.846	6,78%
Servicios sociales	**599**	7.287	8,22%
Justicia	**492**	10.112	4,87%
Hacienda pública y gestión de administraciones tributarias	**419**	9.009	4,65%
Gestión sancionadora	**373**	4.043	9,23%
Gestión y control sanitario	**371**	3.566	10,40%
Padrón de habitantes	**308**	5.503	5,60%
Trabajo y gestión de empleo	**307**	4.711	6,52%
Gestión económica-financiera pública	**300**	5.995	5,00%
Prevención de riesgos laborales	**283**	1.249	22,66%
Seguridad y control de acceso a edificios	**278**	2.219	12,53%
Historial clínico	**244**	1.894	12,88%
Videovigilancia	**237**	434	54,61%
Publicaciones	**207**	1.390	14,89%
Seguridad pública y defensa	**194**	3.178	6,10%
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	**154**	2.539	6,07%
Investigación epidemiológica y actividades análogas	**131**	1.740	7,53%
Prestación de servicios de certificación electrónica	**89**	1.351	6,59%
Gestión del censo poblacional	**79**	296	26,69%
Otras finalidades	**3.771**	17.613	21,41%

TRANSFERENCIAS INTERNACIONALES DE DATOS

Resoluciones de autorización

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total Auto.
Estados Unidos	1	9	2	6	40	9	16	10	31	**26**	**152**
Latinoamérica											**132**
Panamá	-	-	-	-	-	2	-	-	-		**2**
Colombia	-	-	-	-	-	1	4	9	4	**12**	**30**
Chile	-	-	-	-	-	1	7	9	1	**8**	**26**
Uruguay	-	-	-	-	-	1	1	1	4	**3**	**10**
Perú	-	-	-	-	-	-	4	5	4	**19**	**32**
Guatemala	-	-	-	-	-	-	1	-	1	**1**	**3**
Paraguay	-	-	-	-	-	-	1	1	4	**4**	**10**
Brasil	-	-	-	-	-	-	-	1	3	**-**	**4**
El Salvador	-	-	-	-	-	-	-	1	-	**-**	**1**
Costa Rica	-	-	-	-	-	-	-	1	1	**-**	**2**
Nicaragua	-	-	-	-	-	-	-	1		**-**	**1**
México	-	-	-	-	-	-	-		3	**8**	**11**
India					4	-	3	2	30	**28**	**67**
Otros países											**77**
Marruecos	1	-	-	-	2	2	2	1	3	**8**	**19**
Singapur	-	-	-	-	1	-	1	2	-	**-**	**4**
Japón	-	-	-	-	-	1	-	1	-	**1**	**3**
Malasia	-	-	-	-	-	1	1	1	-	**3**	**6**
Tailandia	-	-	-	-	-	1	-	1	-	**-**	**2**
Filipinas	-	-	-	-	-	-	3	1	5	**4**	**13**
China	-	-	-	-	-	-	1	1	3	**3**	**8**
Hong Kong	-	-	-	-	-	-	1	-	-	**1**	**2**
Egipto	-	-	-	-	-	-	-	1	-	**-**	**1**
Nigeria	-	-	-	-	-	-	-	1	-	**-**	**1**
Túnez	-	-	-	-	-	-	-	1	-	**-**	**1**
Sudáfrica	-	-	-	-	-	-	-	-	3	**-**	**3**
Australia	-	-	-	-	-	-	-	1	-	**7**	**8**
Canadá	-	-	-	-	-	-	-	1	-	**-**	**1**
Rep. Bielorrusa	-	-	-	-	-	-	-	-	3		**3**
Mónaco	-	-	-	-	-	-	-	-	-	**1**	**1**
Israel	-	-	-	-	-	-	-	-	-	**1**	**1**
Solicitudes presentadas	2	9	2	19	56	45	54	127	137	**166**	**617**
Archivadas	-	-	-	13	6	16	17	68	42	**20**	**182**
TOTAL AUTO.	**2**	**9**	**2**	**6**	**47**	**19**	**46**	**43**	**103**	**128**	**405**

FICHEROS DE VIDEOVIGILANCIA

AÑO DE INSCRIPCIÓN	Titularidad Privada	Titularidad Pública	Total
1994	7	2	9
1995	4	0	4
1996	1	0	1
*1997-1998	0	0	0
1999	3	0	3
2000	12	0	12
2001	15	0	15
2002	27	0	27
2003	79	0	79
2004	109	3	112
2005	242	0	242
2006	422	14	436
2007	4.802	87	4.889
2008	9.252	186	9.438
2009	22.060	286	22.346
TOTAL	**37.035**	**578**	**37.613**

* 1997-1998. Años sin actividad de registro de ficheros de videovigilancia.

FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

ACTIVIDAD PRINCIPAL	Ficheros
Comercio	7.325
Turismo y hosteleria	4.749
Comunidades de propietarios	2.712
Sanidad	2.273
Industria quimica y farmaceutica	1.055
Construccion	1.022
Actividades relacionadas con los productos alimenticios, bebidas y tabacos	997
Transporte	799
Seguridad	698
Actividades inmobiliarias	693
Servicios informaticos	608
Maquinaria y medios de transporte	575
Educacion	559
Sector energetico	505
Actividades relacionadas con los juegos de azar y apuestas	411
Asociaciones y clubes	409
Produccion de bienes de consumo	366
Contablidad, auditoria y asesoria fiscal	363
Servicios de telecomunicaciones	357
Actividades de servicios sociales	309
Actividades diversas de servicios personales	286
Agricultura, ganaderia, explotacion forestal, caza, pesca	276
Entidades bancarias y financieras	226
Actividades juridicas, notarios y registradores	190
Comercio y servicios electronicos	174
Actividades de organizaciones empresariales, profesionales y patronales	129
Seguros privados	122
Organizacion de ferias, exhibiciones, congresos y otras activ. relac.	55
Investigacion y desarrollo (i+d)	50
Inspeccion tecnica de vehiculos y otros analisis tecnicos	50
Publicidad directa	49
Actividades politicas, sindicales o religiosas	42
Actividades postales y de correo (oper. postales, serv. post., transport.	30
Mutualidades colaboradoras de los organismos de la seguridad social	16
Seleccion de personal	12
Solvencia patrimonial y credito	5
Otras actividades	8.538
TOTAL	**37.035**

5. PRESENCIA INTERNACIONAL DE LA AEPD

COMISIÓN EUROPEA

Sesiones Plenarias GT29 en Bruselas – 5

- 10 y 11 de febrero.
- 7 y 8 de abril.
- 16 y 17 de junio.
- 12 y 13 de octubre.
- 30 de noviembre y 1 de diciembre.

Reuniones de Subgrupos en la Comisión Europea (Bruselas) a las que asiste la AEPD – 18

- Subgrupo de Tecnología (22 de enero y 16 de diciembre).
- Subgrupo Cláusulas contractuales (15 de enero).
- Subgrupo Ad Hoc Programa de Trabajo (30 de enero).
- Subgrupo FEDMA (17 de febrero).
- BCR y Safe Harbour, adecuación de terceros paises (18 de marzo y 16 de septiembre).
- Cumplimiento y aplicación de la Legislación ("enforcement") (25 de junio).
- Subgrupo WADA (18 de febrero).
- Subgrupo responsable-encargado (20 de febrero y 25 de septiembre).
- Subgrupo asuntos financieros (30 de junio y 15 de diciembre).
- Subgrupo datos de viajeros (8 de julio).
- Subgrupo de futuro de la privacidad (22 de julio, 4 de septiembre, 6 de octubre y 10 de noviembre).

CONSEJO DE EUROPA

- Reunión del Boureau del Comité Consultivo del Consejo de Europa. (09-10 de febrero, Estrasburgo, Francia).
- Plenario del Consejo de Europa. (3-5 septiembre, Estrasburgo, Francia).

CONSEJO DE LA UNIÓN EUROPEA – 15

- ACC del Convenio de Schenguen (24 de marzo y 23 de junio, Bruselas, Bélgica).
- ACC del Convenio de Europol (23 de marzo y 22 de junio, Bruselas, Bélgica).
- ACC Sistema de Información Aduanero (24 de marzo y 23 de junio, Bruselas, Bélgica).
- ACC Eurodac (25 de marzo y 24 de junio, Bruselas, Bélgica).
- Grupo de Trabajo de Policía y Justicia (24 de marzo y 24 de junio, y Bruselas, Bélgica y 11 septiembre, Roma).
- EUROJUST (12 de febrero, 4 de abril y 23 de junio, La Haya).
- EURODAC (18 de diciembre).

OCDE - 2

- Grupo de trabajo de privacidad y seguridad (10 de marzo, Paris).
- Grupo de trabajo de privacidad y seguridad (13 de octubre, Paris).

GRUPOS DE TRABAJO SECTORIALES - 4

Grupo de telecomunicaciones de Berlín: (2)
- 12 y 13 de marzo, Sofía (Bulgaria).
- 5-6 septiembre, Berlín (Alemania).

Grupo del Taller de Reclamaciones: (1)
- 12 y 13 de marzo, Praga (Rep. Checa).

Grupo de Trabajo de la Comisión sobre Retención de datos
- 3 de diciembre, Bruselas

RELACIONES BILATERALES

Programas de Hermanamiento (Twinnings)

Israel:
En 2008 la Agencia ha sido adjudicataria, tras competir con diversas Agencias de Protección de Datos Europeas, del primer proyecto de hermanamiento entre la UE y el Estado de Israel. El proyecto que va a hermanar a la Agencia con su homóloga Israelí (ILITA) está financiado por la UE con 1 mill. de euros y tiene una duración prevista de 18 meses. Su ejecución ha comenzado en Junio de 2009 y durante este ejercicio se han llevado a cabo las siguientes actividades:
- Realización de una conferencia internacional como inauguración del proyecto en la que se ha abordado la situación de la protección en Europa y en Israel.
- Seminario cuyo objetivo ha sido analizar el marco actual en materia de protección de datos en Israel.
- Definición y realización de una encuesta entre la población Israelí para conocer su grado de concienciación en materia de protección de datos.
- Seminario sobre la definición e implantación de una estrategia de comunicación para la autoridad de protección de datos Israelí.
- Seminario para establecer una metodología común para la realización de diferentes guías sectoriales en Israel.

- Seminario para abordar la problemática del sector de las telecomunicaciones en Europa en general y en Israel en particular. Elaboración de una guía sobre la protección de datos en el sector de las telecomunicaciones en Israel.
- Seminario para abordar la problemática en el ámbito laboral en Europa en general y en Israel en particular. Elaboración de una guía sobre la protección de datos en el ámbito laboral en Israel.
- Realización de una visita de estudio del Comité de Dirección de ILITA a la Agencia con el fin de conocer in-situ su estructura y funcionamiento.

Las actividades anteriores han contado con la participación de expertos de la Agencia española así como de expertos procedentes del sector público y privado del Reino Unido, Francia, Italia, Grecia y Eslovenia.

IBEROAMÉRICA

13 de mayo. Madrid (España)
Seminario "El Derecho a la Protección de Datos Personales: la situación actual en los países iberoamericanos". Se enmarca dentro del Máster Oficial en Derecho de la Facultad de Derecho de la Universidad Alcalá de Henares.

26-28 de mayo. Cartagena de Indias (Colombia)
I Seminario Euro-Iberoamericano de Protección de Datos: "La Protección de los Menores". Coordinado y organizado por la AEPD y la AECID. Con motivo de este seminario se celebró una reunión del Comité Ejecutivo de la Red Iberoamericana para coordinar los temas de actualidad y de organización de futuros eventos.

3 de noviembre. Madrid (España)
Celebración del VII Encuentro Iberoamericano de Protección de Datos en la Casa de América. Asisten representantes de las autoridades de protección de datos, transparencia y acceso a la información pública de 20 países miembros de la Red Iberoamericana. En la jornada de tarde se celebró el I Encuentro entre la Red Iberoamericana de Protección de Datos y la Asociación Francófona de Autoridades de Protección de Datos, asistiendo representantes de 26 países y Principados, miembros de esta Asociación, miembros de la Comisión Europea y representantes del Supervisor Europeo de Protección de Datos.

CONFERENCIAS INTERNACIONALES

- Conferencia Europea de Autoridades de Protección de Datos, 23-24 de abril, Edimburgo.
- Reunión de la Internacional Association of Privacy Professionals (IAPP),12 y 13 de marzo, Washington.
- Taller de la Federal Trade Commission sobre Data Security, 16 de marzo, Washington.
- Conferencia EPOF, 18 de marzo.
- Conferencia Data Breach Notification Laws in Europe, 22 de abril, Edimburgo.

- Conferencia "Personal data - more use, more protection?" 19-20 mayo, Bruselas.
- Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. 4-6 noviembre, Madrid.
- Conferencia sobre "Safe-Harbour- Flujos transfronterizos de datos, protección de datos y privacidad", organizada por el Departamento de Comercio de los Estados Unidos, 16-18 de noviembre.
- Conferencia "The Public Voice – Estándares Globales sobre Privacidad en un Mundo globalizado", 3 de noviembre en Madrid.

VISITAS INSTITUCIONALES

De otras delegaciones a la AEPD

- Visita de representantes del Senado de Francia, 13 de febrero Madrid.
- Visita de la delegación de funcionarios de Bosnia Herzegovina, 2 de junio, Madrid.
- 27 de marzo: Visita Comisionados del Instituto de Transparencia y Acceso a la Información Pública del Estado de México.
- 25 mayo al 19 junio: Pasantía realizada por dos representantes de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).
- 22-23 de junio: Visita de una delegación del gobierno y del Consejo para la Transparencia chileno.
- 15 de julio: Visita del Agregado Comercial de la Embajada de Guatemala en España.
- 17 de julio: Visita de una delegación representativa de diferentes instituciones del gobierno brasileño.

Otras

- High Level Meeting de Propuesta Conjunta de Estándares Internacionales. Barcelona, 12 de enero.
- High Level Meeting de Propuesta Conjunta de Estándares Internacionales. Bilbao, 11 de junio.
- World Anti-Doping Agency- Consejo Superior de Deportes, (23 de abril).
- Reunión sobre Estándares Internacionales de Privacidad con el Supervisor Europeo de Protección de Datos (Bruselas, 8 de julio).
- Reunión sobre Estándares Internacionales de Privacidad con el Supervisor Europeo de Protección de Datos en la CNIL (Paris, 9 de julio).
- World Anti-Doping Agency y CAHAMA Consejo Superior de Deportes, (14 de septiembre, Madrid).
- DG de la Sociedad de la información (15 de octubre, Madrid).
- Reunión Safe Harbour.
- Reunión del Grupo de Trabajo de Standard – Setting, Banco Mundial (22 de septiembre, Madrid).

6. SECRETARÍA GENERAL

RECURSOS HUMANOS

PERSONAL a 31/12/2009	Dotación	Efectivos
	Funcionarios **158**	Funcionarios **147**
	Laborales **8**	Laborales **7**
	Alto Cargo **1**	Alto Cargo **1**

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos 2009	5	3	19	45	2	14	3	12	2	7	12	23

GRUPO	A1	A2	B	C1	C2
Efectivos 2009	27	48	-	23	49

GRUPO	TOTAL
Hombres	67
Mujeres	88

EVOLUCIÓN DEL PRESUPUESTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DURANTE LOS EJERCICIOS 2006 A 2009

CAPÍTULO	Crédito ejer. 2006 (euros)	Crédito ejer. 2007 (euros)	Crédito ejer. 2008 (euros)	Crédito ejer. 2009 (euros)
I	3.896.313,16	3.970.471,82	5.292.866,85	**6.692.929,00**
II	4.626.725,42	5.094.745,78	6.189.248,11	**6.701.771,00**
III	122.400,00	5.998,51	47.555,34	**12.290,00**
VI	1.124.600,00	1.471.340,00	1.900.770,00	**1.900.770,00**
VIII	6.380,00	10.000,00	10.000,00	**10.000,00**
TOTAL	**9.776.418,58**	**10.552.556,11**	**13.440.440,30**	**15.317.760,00**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ANNUAL REPORT 2009

SPANISH DATA PROTECTION AGENCY. CURRENT SITUATION AND FUTURE PERSPECTIVES

< ÍNDICE >

1. A MORE INFORMED SOCIETY MORE CONSCIOUS OF ITS RIGHTS

A. GREATER SOCIAL AWARENESS REGARDING THE RISKS OF INTERNET

In order for citizens to benefit from effective protection in the use of their personal data not only must they know the rights which the regulations recognise for them and the manner in which these may be exercised but they must also keep their degree of awareness "updated" in the light of the new risks that affect their privacy, foremost among which are those generated by technological development and the new Internet services.

The data of the Sociological Research Centre (CIS) barometer for September 2009 on trust in the Internet reveal that 56% of citizens think that security and privacy in the Web is low or very low, confirming that citizen concern regarding the risks of the Internet is a confirmed reality.

The Spanish Data Protection Agency (AEPD), for its part, has redoubled its efforts to improve the knowledge of citizens on this subject and to make measures available to avoid the risks. In this respect, it has carried out a joint study with the National Institute of Information Technologies (INTECO) on the privacy of personal data and security in online social networks and has updated a guide with recommendations to Internet users which analyses the main risks that are currently present in the Web.

But there is no doubt that mass media have played a decisive role in raising citizen awareness, focusing on the impact of new technologies on the privacy of individuals and, specifically, on the risks associated with services such as social networks. The AEPD has recognised this work of dissemination by granting its 2009 communication and dissemination awards to programmes such as "12 months 12 causes" by the television channel Telecinco, the weekly section on data protection on Radio 5 Todo Noticias and a documentary project to inform minors with regard to new technologies.

B. CITIZENS, MORE AWARE OF THEIR RIGHTS

The CIS barometer indicates that citizens have more and more knowledge of their rights. Thus, the concern for data protection and the use of personal information has grown, reaching 74.1% of those surveyed. The percentage of citizens who know of the existence of the Spanish Data Protection Act (LOPD) is around 50%, and the same occurs with the AEPD as the organisation that guarantees their rights, which for the first time exceeds the 50% barrier.

The greater awareness by citizens is resulting in a growing demand for the guarantee of their rights. A significant example is the growth of almost 34% in the number of consultations placed with the Citizen Attention Service, by telephone, in person or in writing, approaching in 2009 the figure of 100,000. Likewise, visits to the web page of the AEPD increased by 700,000 compared to 2008, reaching 3,000,000, which means a daily average of 8,214 visits. The number of consultations of the General Data Protection Register has also experienced considerable growth in the last 12 months, the total figure being around 2.5 million.

The analysis of the consultations placed indicates that video-surveillance has become one of the outstanding concerns of citizens, combined with advertising and credit reporting, or information regarding access to medical records. But other doubts are beginning to gain relevance, regarding what to do so that personal data disappear from a web page, whether it is obligatory to register the geolocation files of employees, or whether Bluetooth scanning which reports information on mobile telephones is included in the LOPD.

A survey by the AEPD reveals that almost 90% of citizens declared that they felt satisfied or very satisfied with regard to the waiting time in order to be assisted and regarding the attention received. The satisfaction index regarding the information received, the knowledge and manner of the helpline operator of the AEPD varies between 99.88% and 100%.

C. NEW CONCERNS: HOW DO I DISAPPEAR FROM A WEB PAGE? MUST I RESIGN MYSELF TO BEING VISIBLE IN THE INTERNET? HOW DO I EXERCISE MY RIGHT TO OBLIVION?

The AEPD observes that the greater knowledge of data protection regulations corresponds with more active behaviour by citizens in the exercise of their rights before those who process their personal information. In this respect, an increase of almost 14% can be appreciated in requests for the safeguard of rights, in the region of 2,000. Requests for erasure of data or object to their processing by Internet browsers, still not very numerous, have increased by 200%.

In the light of the question, Must I bear being visible in the Internet? the reply is no. The decisions pronounced by the AEPD take the line of requiring that the necessary measures be adopted to avoid the indexing of personal data, likewise taking into account the possible actions that webmasters may adopt to make effective the right requested by the individual.

But, aside from these matters, the main questions that citizens continue to ask are: Who has my data? How can I erase them? This is shown by the considerable increase in the decisions relating to the safeguard of the rights of access (59%) and erasure (40,8%), these latter adding up to a total of 1,366 decisions. Another new development is the sharp increase in decisions regarding the right to object (470%).

2. GUARANTEE EFFECTIVE AND EFFICIENT COMPLIANCE WITH THE LOPD

A. FACILITATE COMPLIANCE WITH THE LAW: A GUARANTEE FOR CITIZENS

Informative policy has been intensified in the conviction that facilitating compliance with the law results in an increase in the guarantees to citizens. Thus, in January 2009 the 2nd Annual Open Session was held, which was attended by around 700 participants and the catalogue of practical guides has been expanded, publishing new editions with recommendations to Internet users, video-surveillance and data protection in the workplace and, in English, the guides on video-surveillance and the rights of boys and girls and the duties of fathers and mothers.

The Helpline continues to be a very useful channel in the informative policy of the Agency, as is shown year after year by the increase in consultations. The Legal Department, for its part, attended to a total of 679 consultations, of which 359 (54%) were placed by the Public Administrations and 313 (the remaining 46%) by the private sector.

These policies continue to give results. In 2009, almost 400,000 files were registered in the General Data Protection Register (RGPD), which implies an increase of over 50% compared to 2008, reaching a total figure of 1,647,756. One contribution to this increase has been the simplified file notification system NOTA, which facilitates notification via the Internet, something which is used in almost 90% of manual notifications. Furthermore, the use of digital certificates is gaining ground, to the point that this format is used in one in five notifications.

The increase in registrations is strongest in the private sphere, which has grown by 63%, whilst in the public sector an increase of almost 50% can be highlighted in Local Administration files, owing to which the files of municipalities in the RGPD represent almost 96% of the Spanish population.

The offer of new channels to facilitate compliance with the law has given a qualitative leap in the EVALÚA program, an online self-test for self-assessment of compliance with the LOPD for companies and local authorities, which offers free of charge answers to the doubts which habitually confront those who process personal data.

B. A PERMANENT ZEAL FOR LEGAL CERTAINTY

The AEPD has continued working to achieve greater legal certainty via its mandatory opinions on provisions of general application. 100 provisions have been reported on, such as the draft bills on money laundering and the financing of terrorism, or that of simplification of information and intelligence between the security services of the Member States of the EU. Opinions have also been prepared on the agreements of the EU with Australia and the USA regarding the processing and transfer of EU sourced Passenger Names Records (PNR).

Moreover, the analysis of the degree of legal certainty in the application of the LOPD obliges contemplation of the extent to which the decisions of the AEPD are ratified or revoked by the Courts. In relationship with the appeals regarding the erasure of data in the Baptism Records of the Catholic Church, during 2009 99 rulings have been issued in the first instance by the Spanish National Court (29% of the total) and the Supreme Court has judged 163 appeals (more than 90% of the total) in the sense upheld in its ruling of 19 September 2008.

Not including the rulings mentioned, in 2009 the contentious-administrative chamber of the Spanish National Court and the Supreme Court have issued 240 and 19 rulings, respectively. Regarding the rulings of the National Court:

- 162 dismissed the appeals brought against decisions of the Agency (which were fully confirmed) (68%).
- 17 partially upheld the appeals (7%).
- 61 wholly upheld the claims to set aside the decisions of the Agency (25%).

For its part, and also without referring to the rulings on the Baptism Records of the Catholic Church, the Supreme Court ratified the criteria of the Agency on 16 of the 19 occasions on which the matter was subjected to its judgment.

C. A GROWING DEMAND FOR GUARANTEES: AN ACTIVE RESPONSE BY THE AGENCY

The number of claims brought before the AEPD in 2009 has caused an increase of 75% in the actions brought, exceeding 4,100 (where telecommunications, financial institutions and video-surveillance have been the main sectors investigated).

However, in decisions on sanction procedures against private organisations, telecommunications and financial institutions, despite occupying the first and third place based on the number of proceedings, have decreased by 10.34% and 21.26% respectively. On the other hand, private video-surveillance for security reasons rises to second place, with a 229.55% growth on the previous year. The decisions which declare a breach of the LOPD by the Public Administrations have increased by around 12.5%.

The amount of the sanctions imposed amounted to 24,872,979.72 euros. Although this figure represents an increase of 12.99% compared with the previous year, it is close to the volume of sanctions declared in the year 2006, with the relevant difference that the number of sanction procedures resolved in 2009 is higher than that of 2006 by 235%. It is precisely the considerable increase in sanction procedures and not the sum of the sanctions declared that explains the figure of the sanctions imposed. Minor sanctions are those which present the greatest increase (44.76%), whilst serious ones remain stable and very serious sanctions decrease by almost 6%. Regarding the total of the sanctioning decisions, a qualified reduction of the liability of the offenders can be seen in 40.72% of the cases.

Analysing the data that have been presented it is appropriate to conclude that the quantitative increase in the sanctions, a consequence of the previous increase in complaints, does not hinder appreciation of the improvement in compliance with the LOPD, with the growth in breaches for reasons of form, the reduction of very serious breaches and the reduction of liability when a breach is committed.

The 2008 Annual Report included citizen concern regarding the receipt of advertising by telephone. To give an efficient response to this question, the AEPD has promoted, together with the Spanish Federation of Electronic Commerce and Direct Marketing (FECEMD), a new opt-out file so that those who do not wish to receive advertising may express this and choose the channels via which they wish to receive advertising, whether by post, e-mail, SMS, MMS or telephone. From the information requested from FECEMD the number of persons registered in the Robinson List service amounted to more than 110,000 at 31 December 2009. The implementation of the service is a palpable demonstration of the efficiency of the preventive policies and collaboration with those obliged by the LOPD to increase the guarantees to citizens.

Furthermore, in an environment of economic crisis such as that which developed during 2009, an exponential increase has taken place in actions deriving from or related to claims for default.

Mention must also be given to the very considerable increase in the invoking by citizens of the defence mechanisms granted by the LOPD in the light of undue processing of their personal data in the sphere of creditworthiness. The number of procedures for the protection of data subjects' rights brought on this matter increased by 570% and that of preliminary actions prior to possible sanction proceedings by 225%. In the sphere of the assignment of receivables between companies, also known as sale of debt, various sanction procedures have been resolved which have derived in the imposition of sanctions that have reached up to 420,000 euros. Likewise, it is appropriate to highlight the existence of various complaints against possible practices which violate the duty of secrecy in actions of recovery, via the disclosure of the debt to family members or relatives to force the collection of an allegedly owed sum.

3. PRIVACY AT RISK: THE BIG QUESTION-MARKS

A. INTERNET. NEW SERVICES, NEW CHALLENGES

The consideration for the free use that users make of Internet services is the unilateral establishment of term and conditions by the service provider. Therefore, priority should be given to those active policies aimed to establish relations with the providers of these services. In this respect, the AEPD has communicated to Facebook and Tuenti the recommendations of the study prepared with INTECO, insisting on the improvement of privacy policies so that they offer clear and understandable information, and on the need to set up privacy policies by default and erase all the contents of the profile as soon as unregistration is requested.

In 2009 156 proceedings were brought regarding preliminary proceedings specifically related to services provided via Internet. A new aspect is the fact that 18 of these proceedings were instituted as a consequence of 31 complaints related with users of the social networks Facebook and Tuenti, the majority referring to the dissemination of photographs of third parties without their consent.

The majority of the rest of the actions are also related with the unauthorised dissemination of personal data via Internet: 37 of them refer to forums or blogs, 13 to video hosting services, fundamentally Youtube, and 38 to other types of web site such as corporate sites, collections of law reports or personal sites. Another 28 claims are related to advertisement web sites, online dating services or electronic mail services. In the majority of cases they are related with the unauthorised dissemination of data.

Likewise, 10 of the actions deal with incidents of various types related with online shopping or with electronic commerce operations. Finally, it is appropriate to mention 5 preliminary proceedings brought in relation to web search engine services and the location of personal information in directories or in people search engines.

B. MINORS. A NECESSARY PROTECTION IN THE LIGHT OF THEIR GROWING PRESENCE IN THE WEB

The use of social networks has become a habitual activity for the social development of minors, to whom they offer access to a new means for contacting each other. The risk for them is that, to a great extent, they start out with a basic educational deficit regarding the lack of knowledge of how to exercise real control over their information.

Data protection regulations do not allow minors under the age of fourteen to register as users of a social network without the consent of their parents. The Agency has assumed compliance with this obligation as a priority. In fact, in the meetings held with those responsible for Tuenti and Facebook, the control of access by minors has been a permanent demand.

In reply to the demands of the AEPD, Tuenti presented an age verification system that analyses the profiles of suspect users, erasing those who do not prove that they are 14 years old. Likewise, it has undertaken to strengthen the purging processes of existing profiles and to develop systems for the verification of new suspect profiles. Furthermore, it has issued information regarding the modification of the privacy policy, establishing by default the maximum level of privacy for users under the age of 18. Likewise, the Agency requested those responsible for Facebook to increase the age limit to 14 years for users in Spain.

However, it is necessary to incorporate in syllabi adequate training on data protection and privacy, as well as for Public Administrations and schools to make technologies available to pupils that limit access to Web services by the under-14s. In this context, the electronic Identity Document is proving to be one of the most efficient instruments for accrediting age in the Internet. This Agency considers it to be extremely important that the adequate initiatives be implemented in order for over-14s to have the digital means available to allow them to prove that they have the required age to give their consent to the processing of their data.

C. VIDEO-SURVEILLANCE: LIVING WITH GUARANTEES

Video-surveillance for security reasons has become an omnipresent reality. Each year significant growth takes place of video-surveillance files, as in 2009, when the files registered in the General Data Protection Register which declare this purpose increased by around 240% in the private sphere exceeding the figure of 37,000. In the public sphere the increase was 60% with a total of 578 files.

The 2009 survey of the CIS reflects that 68.7% of citizens are in favour of their installation, whilst 10% are against. However, more and more people lodge complaints of breaches of the LOPD in relationship with video-surveillance, where the sanction procedures resolved have increased by 230%.

Furthermore, the recent enactment of the Act 25/2009, of 27 December, for the modification of various laws for their adaptation to the Act on free access to service activities, has extended the legitimisation for the installation and use of video-surveillance devices. This will presumably give rise to a reduction of the sanctioning decisions of the AEPD, the said fault of legitimisation being one of the most frequent breaches.

Regarding cameras that allow images to be transmitted via the Internet, the AEPD carried out a sectoral inspection, noting that the majority allow identification of the persons filmed. The main deficiency detected is that, habitually, the control mechanisms for access to the images are disabled by the manufacturer or are activated with a default username and password. The lack of diligence in access control causes a vulnerability that allows access by third parties by leaving the camera in an "open door" situation. A catalogue of recommendations is offered, among them the need to activate the control of access to the images with username and password. The inspection has led to the bringing and resolution of 7 sanction procedures.

D. EMPLOYMENT CONTEXT: BALANCE BETWEEN RIGHTS AND OBLIGATIONS

The variety of processing of personal data carried out in the employment sphere has led the AEPD to prepare a guide on data protection in companies, to provide an answer to practical aspects which companies must habitually confront, suggesting criteria that allow compliance with personal data protection regulations. The guide includes specific recommendations on the processing of specially protected data, in particular, those on health and trade union membership, as well as the guarantees that should be observed in occupational risks-prevention.

Although not necessarily dealing with personal data, it also incorporates recommendations so that the implementation of internal whistleblowing schemes in the company is carried out while guaranteeing the protection of the employees. The chapter dedicated to employer controls indicates the rules applicable to biometric controls, video-surveillance in the workplace or on the use of technological tools provided by the employer and, also, those related to the control of occupational absenteeism.

E. INTERNATIONAL DATA FLOWS. FLEXIBILITY AND GLOBALISATION

International data transfers from Spain have globalised and reach all the geographical areas of the world. The number of authorisations increased by 25%, the USA being the first destination country, despite the reduction in the number of transfers. Strong growth can be seen of over 100% to Latin-American countries (132 authorisations), whilst Asia maintains a constant volume of authorisations (115). In the African continent international transfers focus on Morocco (19) and the Republic of South Africa (3) and Australia appears as an emerging destination

The search for more flexible procedures for the authorisation of international transfers has advanced in 2009. The AEPD authorised the first transfer based on binding corporate rules (BCR) and has participated via a coordinated procedure in ten requests with this type of guarantee presented before other Authorities of the European Union.

To conclude, it can be affirmed that we are witnessing a constant increase in international data flows with a great weight of the delocalisation of services and with more flexible authorisation procedures. From this we can deduce the urgent need to achieve binding standards to guarantee the protection of privacy in a globalised world.

4. 2009: MADRID, WORLD PRIVACY CAPITAL. THE MADRID RESOLUTION: A MEETING POINT FOR A GLOBAL REGULATION

In 2009 the AEPD organised the 31st International Conference of Data Protection and Privacy Authorities – the largest forum dedicated to privacy at world level and a meeting point between data protection authorities and guarantors of privacy from the whole planet, as well as representatives of public and private bodies and civil society – converting Madrid into the world privacy centre between 2 and 6 November. It was attended by more than 1,000 people from 83 countries.

This Conference, inaugurated by their Highnesses the Prince and Princess of Asturias, took place in the Congress Palace of Madrid, under the slogan "Privacy: today is tomorrow". The nearly one hundred speakers, divided into twenty sessions, included the Spanish Interior Minister, Alfredo Pérez Rubalcaba and the Secretary of Homeland Security of the United States, Janet Napolitano, Martin Cooper (inventor of the mobile telephone), Vinton Cerf (co-inventor of the TCP/IP family of Internet protocols) as well as the Minister of Industry, Commerce and New Technologies of Morocco, Ahmed Reda Chami. However, the greatest achievement of this edition has been to manage to advance towards a universal and binding legal instrument on the subject of privacy, that contributes to a greater protection of individual rights and freedoms in a globalised world and which benefits from the widest institutional and social consensus.

Via the adoption of the designated "Resolution of Madrid", a large step was taken along this line: the "Joint proposal for a Draft of International Standards for the Protection of Privacy with regard to the Processing of Personal Data". This proposal aims, on the one hand, to promote the right to data protection and privacy internationally, offering a model of regulation that guarantees a high level of protection and which, at the same time, may be assumed in any country; on the other hand, it seeks to facilitate the flow of personal data at international level, trying to mitigate the existing obstacles.

Despite not being an international agreement or a legally binding regulation, its value as a reference text is justified not only by the ample participation of the international data protection and privacy community in its preparation, but also because it includes elements that are present in all the valid data protection systems currently in force, as well as by the fact that it has been backed by all the Authorities that attended the International Conference. Therefore, the promotion and dissemination of this text among private bodies, experts and national and international public organisations will be one of the priorities of the AEPD during the year 2010.

5. KEYS FOR THE DEVELOPMENT OF A NEW EUROPEAN PRIVACY FRAMEWORK

A. TREATY OF LISBON

The Treaty of Lisbon, which came into force on 1 December 2009, includes the Charter of Fundamental Rights of the European Union, which recognises, reinforces and makes binding the rights, freedoms and principles of the Member States of the Union. The Charter contains two articles on the subject of privacy and data protection which mark an important consolidation of the data protection legislation of the UE.

Among other new innovations it creates a common framework for all the activities of the Union, abolishing the old division, this change of structure also being reflected in the data protection sphere. Until now, although data protection benefited from harmonisation in the sphere of the first pillar of the European Community, it was not so in the activities carried out in the framework of the third pillar, that relative to police and legal cooperation on criminal matters. In summary, the new legal framework of the EU is a challenge for the data protection authorities, which will have to review the rules in force and assess the legislators in the taking of decisions in the new fields of activity.

B. STOCKHOLM PROGRAMME

The Stockholm Programme on the European Area of Freedom, Security and Justice was approved in the last meeting of the Council of Ministers of the Swedish Presidency of the European Union, on 12 and 13 December. This Programme recognises the protection of the fundamental rights and, in particular, the protection of personal data. It also establishes that the EU should have a single system of personal data protection that includes a European certification model for technologies, products and services that protect privacy.

In this line, the Conference of European Data Protection Authorities, held in Edinburgh in April 2009, concluded that it is necessary to review the European data protection framework and analyse the legislation in a globalised world, where the use of Internet and the development of electronic commerce and electronic government are centred on personal information.

C. FUTURE OF PRIVACY

The foreseeable repercussion, on the European legal framework on the protection of personal data, of the coming into force of the Treaty of Lisbon and the Stockholm Programme, is revealed in the implementation by the European Commission of a project to analyse future advances in the development of this fundamental right, which was followed by a public enquiry into its legal framework.

The Article 29 Working Party has prepared a document called "The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data", in which the European Authorities, and among them the AEPD, coincide in pointing out that the validity of the basic principles included in current legislation on the subject of data protection is beyond all doubt, despite the institutional, technological and social changes. However, they also consider that the current legal framework can be improved with regard to its practical application.

During 2010 a group of experts will be convened who will issue a report in which they will set out the possible improvements that, in their opinion, should be introduced in community legislation on the subject of data protection.

6. RECENT INTERNATIONAL DEVELOPMENT

A. ONLINE SOCIAL NETWORKS

In the month of June, the Article 29 Working Party (WP29) approved the Opinion on online social networking, distinguishing under which circumstances it can be considered that the users are taking part in a purely personal or household activity and, therefore, are not subject to obligations on the protection of personal data, or when they may be liable for the information published.

In this respect, it considers that household exemption will not be applied when the social network is used as a collaboration platform for an association or a company, or when access to the information of the profile goes beyond self-selected contacts. In particular, when all the members who belong to the social network can access a profile or when it is possible to access the data using search engines, it is considered that access exceeds the personal sphere. Lastly, the application of household exemption is also limited by the need to guarantee the rights of third parties, especially with regard to sensitive data in the personal or household sphere. In cases in which the domestic exemption is not applicable, the users themselves may be responsible for breach of the LOPD.

On the other hand, the WP29 points out that the providers of social network services who, in many cases, develop applications for them, are responsible for the personal data that they handle, and, in that respect, they have a responsibility towards the users. In this context, it considers that all the necessary measures aimed at adequately protecting the information published on their platforms should be applied.

B. PRIVACY CODE OF THE WORLD ANTI-DOPING AGENCY

The preparation, by the World Anti-Doping Agency (WADA-AMA), of standards in privacy and data protection aimed at covering the processing carried out in the fight against doping, was another of the subjects tackled by the Article 29 Working Party. In its Opinion 4/2009 it concludes that the version adopted required a series of improvements in aspects such as the presumable lack of freedom of the sportsmen and women when consenting to the processing of their data, in the framework of anti-doping controls, the retention periods of the data of the analyses performed and the inexistence of an efficient procedure for the control of compliance with the standard.

After a series of meetings, WADA-AMA adopted a new version of its standards, incorporating a large number of the suggestions contained in the opinion of the WP29. The different improvements introduced contributed to their being better adapted to the levels of protection required by Spanish and Community legislation and, consequently, to a greater protection of the data used for the prevention of doping at world level.

C. OPINION ON THE PROPOSALS AMENDING OF DIRECTIVE 2002/58/EC

The WP29 formulated Opinion 1/2009 on the proposals amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. The document expressed their concern regarding other matters, such as the notification of security breaches and its expansion to information society services, types of breaches that should be notified, persons to whom these breaches can be notified or the affirmation that traffic data are subject to data protection legislation.

D. THE IBERO-AMERICAN DATA PROTECTION NETWORK

The activity of the Ibero-American Data Protection Network has centred on the development of the strategic lines marked in the 6th Meeting of 2008. From the organisational point of view, in May a meeting was held in Cartagena de Indias of the Executive Committee of the Ibero-American Network and the specific web site of the Network has been designed, in operation since November 2009. In addition, the 7th Meeting of the Network was held during the days prior to the 31st International Conference.

7. COOPERATION WITH THE AUTONOMOUS COMMUNITY DATA PROTECTION AGENCIES

The collaboration between the Agencies in 2009 had as its main milestone the holding in Madrid of the 31st International Conference of Data Protection and Privacy. In fact, the Autonomous Agencies collaborated actively with the AEPD in the preparation of the "Joint proposal for a Draft of International Standards for the Protection of Privacy with regard to the Processing of Personal Data" and their directors intervened as speakers in various working sessions of the 31st Conference.

8. RECOMMENDATIONS

A. REGULATORY

- Modify the regulations of the electronic identity card so that minors may authenticate themselves electronically although not sign electronically.

B. EXECUTIVE

- Take every precaution in the exercise of the work of recovery of debts for the complete safeguard of the professional secret regarding the data of the alleged debtors.
- Promotion by Professional Associations of mechanisms that allow the deposit of the information of the data subjects in the case of death or disappearance of data controllers corresponding to their professional sphere.
- The inclusion in primary and secondary school syllabi of training on data protection, privacy and Internet, as well as making available to pupils computer tools that prevent access by under-14s to Internet services for which the consent of their parents or guardians is required.

D.L.: M-22850-2010

Diseño Gráfico: www.ardifusion.com
Impresión: www.cpg.com