AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2013

ISSN 2254-6936
Depósito Legal: M-23875-2014

Imprenta Nacional
Agencia Estatal Boletín Oficial del Estado

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2013

PRÓLOGO

La Memoria de la Agencia Española de Protección de Datos que tengo el honor de presentar ofrece una exposición detallada de las actividades desarrolladas durante el año 2013, enmarcada en un examen del estado actual de la protección de los datos personales y el análisis de cómo se están afrontando los principales desafíos presentes y futuros, tanto en el ámbito nacional como en el supranacional.

El año 2013 ha sido particularmente revelador de los riesgos y las amenazas que se ciernen sobre la vida privada de las personas en las sociedades actuales, altamente tecnologizadas y globalmente conectadas, donde cada día se hace un uso más intenso de la información de carácter personal. Con el continuo desarrollo de las nuevas tecnologías se multiplican no sólo el volumen de datos generados sino también las capacidades técnicas de recopilar, almacenar, analizar y utilizar la información de carácter personal con fines muy diversos. Como consecuencia de ello, se amplían las posibilidades de explotación comercial de los datos personales y se eleva su valor económico. En paralelo, se está produciendo un preocupante fenómeno de concentración de ingentes cantidades de información personal en manos de unos pocos actores globales, que tienen la capacidad de combinar y analizar datos procedentes de fuentes muy diversas, con el consiguiente poder de incidir sobre las conductas de los individuos e incluso de configurar la evolución de las sociedades. La percepción de estos riesgos se ha agravado tras desvelarse las prácticas de recopilación y almacenamiento masivo de información personal por parte de las agencias de seguridad y los servicios de inteligencia de Estados Unidos y de varios países europeos que, entre otras fuentes, se han servido también de los enormes silos y flujos de información que atesoran y gestionan las grandes compañías internacionales proveedoras de servicios en internet.

Todo ello ha provocado que nos encontremos en un periodo crítico para la protección de la privacidad, en el que el impacto de las tecnologías en la esfera privada de los individuos se está agravando y puede erosionar progresivamente la libertad de las personas si no se actúa con celeridad y determinación para corregir la evolución actual. Al igual que en otros momentos históricos en los que se han dado situaciones de amenaza para los derechos individuales, la solución pasa por reforzar las garantías legales y fortalecer las instituciones encargadas de proteger a los ciudadanos. Es necesario reforzar la protección y las garantías para que el poder de autodeterminación sobre nuestra información personal que nos concede el derecho fundamental a la protección de datos se pueda ejercer con eficacia también en internet y en los entornos digitales. Dada la importancia creciente que estos entornos están adquiriendo en nuestras vidas, si los individuos perdemos la capacidad de control sobre la utilización de nuestra información personal en el mundo digital se irá vaciando progresivamente el contenido del derecho fundamental a la protección de datos personales y, con ello, se debilitarán también otros derechos que contribuye a proteger como el derecho a la intimidad, el derecho al honor, la libertad ideológica, la libertad religiosa, el derecho a la no discriminación y, en última instancia, la propia dignidad de la persona.

En este sentido urge que se concluya el proceso de aprobación de un nuevo marco normativo para la protección de datos en Europa. La lentitud con la que se están tramitando las propuestas de Reglamento y de Directiva presentadas por la Comisión en el ya lejano enero de 2012 está generando un grave perjuicio a los ciudadanos y causando serias dificultades a las Autoridades de protección de datos, que se ven obligadas a operar con una normativa que ha sufrido una fuerte erosión desde su aprobación como consecuencia del desarrollo tecnológico y los procesos de globalización. Aunque los principios de la Directiva del año 1995 continúan siendo válidos, muchos de sus preceptos han de ser revisados y actualizados para adaptar el régimen de garantías del derecho fundamental a las nuevas realidades, estableciendo un nivel de protección coherente en todos los Estados de la Unión.

Entretanto, las Autoridades de protección de datos de los Estados Miembros hemos reforzado la coordinación en el seno del Grupo del Artículo 29 con el doble objetivo de lograr el mayor grado posible de armonización en

la interpretación y aplicación de la Directiva y el de hacer frente de modo concertado a los desafíos de las grandes corporaciones internacionales. De lo primero son buena muestra los múltiples documentos elaborados y publicados por el Grupo en los últimos meses sobre temas de actualidad, incluidos los Dictámenes en los que se fijan criterios interpretativos sobre cuestiones centrales del sistema europeo de protección. En cuanto al segundo objetivo, la coordinación entre Autoridades para exigir a las corporaciones internacionales el respeto de la normativa europea ha dado un salto cualitativo con las actuaciones acordadas en el Grupo frente a la contumaz negativa de la empresa Google a adecuar sus políticas de privacidad y el tratamiento de los datos personales de sus usuarios a las normas europeas, que ha dado lugar a una investigación conjunta y a la posterior apertura de procedimientos sancionadores en Alemania, España, Francia, Holanda, Italia y Reino Unido por recopilar y tratar información personal vulnerando la legislación de protección de datos.

En lo que concierne al fortalecimiento institucional como segunda línea de actuación para hacer frente a los retos actuales, en el caso de España, como he señalado en mi comparecencia en la Comisión Constitucional del Congreso de los Diputados, el fuerte crecimiento de la carga de trabajo experimentado en los últimos años ha situado actualmente a la Agencia en una situación de grave dificultad para continuar cumpliendo eficazmente con sus funciones. Al continuo incremento de los asuntos se ha venido a sumar que el legislador le ha atribuido nuevas tareas en materias tan complejas como la normativa de cookies y las brechas de seguridad y que ha asumido íntegramente las competencias de la extinta Agencia de la Comunidad de Madrid sin ninguna compensación, ni en recursos materiales ni personales. Ello ha tenido como consecuencia que la carga de trabajo haya crecido en más de un 200% de promedio (en algunas áreas se supera ampliamente el 300%) desde que en el año 2008 tuvo lugar la última ampliación de plantilla. El reto que este constante incremento ha supuesto para la institución se ha abordado, en parte, mediante la simplificación de los procesos de gestión y recurriendo al uso intensivo de las herramientas informáticas y de las tecnologías de la información pero, sobre todo, gracias a la contribución de los funcionarios que han aceptado esfuerzos adicionales con un alto grado de compromiso y eficacia. Pero la capacidad de asumir más carga de trabajo mediante la optimización de los recursos y la mayor dedicación de los empleados tiene un límite y en el caso de la Agencia no sólo se ha alcanzado, sino que se ha superado. Resulta por tanto ineludible abordar con urgencia un proceso de actualización de la plantilla para que la Agencia pueda continuar desempeñando eficazmente su función de velar por la protección de los datos personales de los ciudadanos en los próximos años, en los que además tendrá que afrontar retos tan complejos como los que plantean, por ejemplo, el big data, la denominada internet de las cosas, o el uso de los drones, tecnologías con un fuerte impacto en la esfera de la vida privada de las personas.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos

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

ÍNDICE

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA 2013

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

1 CIUDADANOS MÁS Y MEJOR INFORMADOS

La información es uno de los elementos fundamentales para que los ciudadanos conozcan los derechos que les reconoce y garantiza la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). El Servicio de Atención al Ciudadano, tanto en su versión presencial como online, es el primer punto de encuentro entre quienes quieren conocer o resolver cualquier duda sobre el derecho fundamental a la protección de datos personales y la Agencia Española de Protección de Datos (AEPD), el ente público independiente encargado de velar por el cumplimiento de la legislación.

Este Servicio ha complementado los tradicionales canales de acceso telefónico, postal y presencial con la posibilidad de presentación de consultas a través de la Sede Electrónica de la AEPD que, puesta en marcha en 2012, se ha consolidado en el ejercicio 2013. Este sistema de consultas dirigido al ciudadano se completa además con la información disponible en la página web de la Agencia.

La Sede Electrónica ha venido a reforzar la web de la Agencia como principal canal de comunicación y relación de la Agencia con los ciudadanos y con los sujetos obligados al cumplimiento de la LOPD, aspecto este último que se detallará con posterioridad en esta Memoria.

Ambas, Sede y web, se han integrado para ofrecer servicios ágiles y sencillos destinados a ayudar a los ciudadanos en el ejercicio de sus derechos y para facilitar a responsables y encargados de tratamiento el cumplimiento de las obligaciones exigidas por la normativa de protección de datos con una disponibilidad permanente.

El principal elemento de la Sede es el registro electrónico, que permite la presentación de documentos electrónicamente siempre que la persona que va a realizar el envío de documentos disponga de un certificado de firma electrónica como medio de identificación.

Por otra parte, es posible obtener información para resolver las dudas que se le puedan plantear a un ciudadano sobre el ejercicio de sus derechos, o herramientas que van a facilitar al responsable que pueda cumplir con los requerimientos de la ley.

El ciudadano dispone de guías para conocer el contenido del derecho fundamental a la protección de datos, vídeos tutoriales que le pueden ayudar a gestionar su privacidad en el uso de internet, procedimientos electrónicos, así como formularios para consultar sus dudas, solicitar el ejercicio de los derechos ARCO, o presentar reclamaciones o denuncias.

Los accesos a la página web de la Agencia se han acercado a los cinco millones (4.985.648), lo que supone un incremento del 21,7% respecto al año anterior y un promedio diario de 6.842 visitas. Por su parte, la *Guía del ciudadano: el derecho fundamental a la protección de datos*, uno de los documentos más consultados, ha tenido 215.299 descargas. Las nuevas funcionalidades de la Sede permiten acceder en primer lugar a un amplio catálogo de preguntas en las que se puede obtener respuesta acerca de las dudas más frecuentes, que se puede completar con el envío de una consulta dirigida al Área de Atención al Ciudadano mediante un formulario disponible en la Sede Electrónica.

La ampliación de opciones para obtener información útil de la Agencia ha dado lugar a variaciones en la distribución de las consultas planteadas por los ciudadanos. Mientras que el volumen de consultas a través de los canales tradicionales ha tenido una disminución del 8.81%, el nuevo sistema de presentación de consultas a través de la Sede Electrónica está asentándose con fuerza.

<Índice>

Las consultas de ciudadanos atendidas a través de los medios convencionales en 2013 han ascendido a 102.064, de las cuales por vía telefónica se han realizado 92.942 —siendo las más frecuentes las relativas a inscripción de ficheros (26.257) y ejercicio de derechos (7.883)—, se han atendido presencialmente 3.817 consultas; y 5.305 se han respondido por escrito —siendo los temas más frecuentes los relativos a cesión de datos (740) y ejercicio de derechos (640)—. Del número total de consultas atendidas por escrito, 4.637 se han presentado ya en 2013 a través de la Sede Electrónica. Adicionalmente, a través de la Sede se han producido 105.092 consultas mediante el sistema de preguntas frecuentes citado con anterioridad.

Es necesario destacar el interés de los ciudadanos en relación con el ejercicio de sus derechos ARCO. Se han recibido, en total, 4.916 consultas, de las cuales 2.535 corresponden al derecho de cancelación, 1.098 al derecho de acceso, 1.018 al derecho de oposición y 159 al derecho de rectificación.

En la distribución de consultas sobre el ejercicio de derechos se aprecia que los ciudadanos plantean cada vez con mayor frecuencia cuestiones sobre el ejercicio del derecho de cancelación, lo cual revela una creciente preocupación en la ciudadanía por conseguir que quienes tratan ilegítimamente su información personal dejen de hacerlo. Esta inquietud sobre el cese en el tratamiento de sus datos personales se ha visto complementada con un interés creciente sobre las opciones que les permiten reaccionar frente a la difusión universal y permanente de su información personal por parte de los motores de búsqueda de internet, ejercitando el denominado «derecho al olvido», que se ha consolidado como uno de los principales temas de consulta a la AEPD.

En relación con las consultas atendidas desde el Área de Atención al Ciudadano, debe señalarse que en 2013 un 95,3% han sido contestadas dentro del plazo de 20 días que figura como compromiso de la Agencia en su Carta de Servicios, y que se trabaja de forma constante para alcanzar el objetivo del 100%.

La importancia de la percepción y, con ello, de la utilidad que tiene para los ciudadanos el servicio de consulta a la Agencia hace necesario su seguimiento

para conocer sus posibles deficiencias y las posibilidades de mejora. Para ello, como en años anteriores, en 2013 se han realizado encuestas de satisfacción dirigidas a evaluar tres aspectos: la satisfacción con el contenido de la información recibida, la valoración de los conocimientos técnicos de la persona que les atendió y la corrección en el trato recibido.

El resultado de las encuestas refleja que prácticamente la totalidad de las personas que se han dirigido al Servicio de Atención al Ciudadano han quedado satisfechas (el 97,4% de los consultados se mostraron satisfechos con la información recibida, el 98,11% consideraron que la persona que les atendió tenía conocimientos suficientes sobre la materia objeto de consulta, y el 98,63% estimaron que el trato recibido fue correcto).

La constatación de los niveles de satisfacción del Servicio de Atención al Ciudadano derivada de las encuestas se ha visto ratificada con la concesión a la AEPD del premio Platinum Award Contact Center al mejor servicio de Atención al Ciudadano de las Administraciones Publicas en el año 2013. Este premio ha sido un motivo de especial satisfacción, en primer lugar, por el reconocimiento a la propia institución y, en segundo término, porque con este galardón también se ha reconocido la labor y el mérito de las personas invidentes que desempeñan su trabajo en el Servicio de Atención al Ciudadano.

En esta labor de dar a conocer el derecho fundamental a la protección de datos cobra también una especial relevancia la difusión que realizan los medios de comunicación de la normativa y sus implicaciones, un elemento que resulta imprescindible para contribuir, por un lado, a crear una sociedad más consciente de sus derechos y, en consecuencia, más libre y, por otro, a avanzar en que empresas y organizaciones sean respetuosas con los datos personales que tratan.

La AEPD ha establecido entre sus prioridades la atención personalizada a los medios de comunicación, que no sólo cumplen una esencial función informativa sino también analítica. Desde el punto de vista cuantitativo, el Gabinete de comunicación ha atendido casi 400 demandas de información y solicitudes de entrevista realizadas por los medios, a las que hay que sumar la elaboración de un total de 30 notas de prensa y convocatorias y 19 notas de agenda informativa e informes en profundidad sobre materias de especial relevancia.

<Índice>

Desde una perspectiva cualitativa, hay que destacar una ampliación en la temática de las cuestiones planteadas por los medios. Así, junto a materias que han seguido acaparando el interés de los medios como la videovigilancia, la cancelación de datos personales en buscadores de internet (el denominado «derecho al olvido») o la inserción indebida en ficheros de solvencia patrimonial y crédito, se han planteado nuevas cuestiones ligadas fundamentalmente al impacto de la tecnología en la privacidad y a la relación entre esta y la seguridad. Algunas de ellas son las siguientes:

- Difusión de datos personales sin consentimiento en redes sociales y otros servicios de internet.
- Fórmulas para concienciar y educar a los jóvenes en el uso tanto de su propia información personal como de terceros en la Red.
- Nuevo marco normativo europeo de protección de datos.
- Cookies y tecnologías de análisis y monitorización online.
- Derecho a la protección de datos en el ámbito laboral.
- Actuaciones y procedimiento sancionador en relación con la política de privacidad de Google en el marco de una acción coordinada junto a las Autoridades de Protección de Datos de Alemania, Francia, Holanda, Italia y Reino Unido.
- Dictamen del Grupo de Autoridades Europeas de Protección de Datos (GT29) sobre la incidencia y los riesgos que plantean las aplicaciones móviles para la protección de datos y la privacidad.
- Comunicado del GT29 sobre el programa PRISM.

A estas materias hay que añadir las acciones de comunicación específicas relacionadas, en gran medida, con la celebración de eventos y presentación de proyectos de la Agencia Española de Protección de Datos:

- **Jornada «20 años de la protección de datos en España»**

El 28 de enero de 2013 la AEPD celebró la jornada «20 años de la protección de datos en España», un evento coincidente con la celebración del Día Europeo de la Protección de Datos. La conmemoración de este aniversario estuvo orientada a realizar un análisis de la evolución de la protección de datos en España, con la participación de destacadas personalidades que representaron a todos los agentes que han participado activamente en el desarrollo de este derecho fundamental en nuestra sociedad.

- **5ª Sesión Anual Abierta de la AEPD**

El 26 de abril de 2013 se celebró la 5ª Sesión Anual Abierta de la AEPD en el Teatro Real de Madrid. La Sesión Anual se ha consolidado como un escenario adicional de comunicación entre la Agencia

<Índice>

y las entidades públicas y privadas, así como con expertos, en el que los asistentes pueden realizar intervenciones y plantear consultas. La celebración de esta cita periódica genera gran interés entre los medios de comunicación ya que, además del análisis sobre la actividad de la Agencia, también se exponen y analizan los retos que actualmente tiene la protección de datos en nuestra sociedad. La 5ª Sesión fue el escenario escogido para la presentación de la *Guía para clientes que contraten servicios de Cloud computing*, un documento práctico dirigido a pymes, profesionales y administraciones públicas que recoge, entre otros aspectos, cómo contratar estos servicios conforme a la normativa de protección de datos. En paralelo, la AEPD también presentó la publicación *Orientaciones para los prestadores de servicios de Cloud computing*, que explica las garantías que deben cumplir los proveedores. En la misma sesión, se presentó el contenido de la *Guía sobre el uso de cookies,* de la que se da cuenta en otro apartado de esta Memoria.

■ Entrega de los Premios Protección de Datos 2012 (XVI edición)

Durante la celebración de la 5ª Sesión Anual Abierta tuvo lugar la entrega de los Premios Protección de Datos correspondientes a 2012 en las categorías de Comunicación e Investigación, que reconocen la indispensable labor realizada por periodistas, medios de comunicación e investigadores en la promoción de este derecho.

El premio principal en la categoría de Comunicación recayó en el programa de RTVE Informe Semanal por la realización del reportaje 'El rastro digital'. Asimismo, se otorgó un accésit a Elmundo.es por sus artículos dedicados a, entre otros temas, el derecho al olvido o la reforma del marco europeo de protección de datos.

En la categoría de Investigación, el jurado concedió el premio principal al trabajo *Algunas consideraciones sobre el Cloud computing*, mientras que los accésit se concedieron a *Análisis de la videovigilancia con fines de seguridad privada en el marco de la protección de datos de carácter personal* y *Derecho de protección de datos y medios de comunicación*. En la modalidad de Investigación sobre el derecho a la protección de datos en países iberoamericanos, se entregó un accésit al trabajo *Derecho fundamental a la protección de datos personales en México*.

■ Día de internet 2013

La AEPD, que forma parte del Comité de Impulso de esta efeméride (17 de mayo), celebra esta iniciativa haciendo un llamamiento para recordar a los ciudadanos la importancia de proteger adecuadamente sus datos personales en la Red. Para ello, dispone de un microsite en su página web que incluye información clara, sencilla y práctica sobre las medidas y precauciones que debe tener en cuenta el ciudadano para navegar por internet, utilizar servicios o instalar aplicaciones de forma segura.

■ Curso Retos para la protección de datos (UIMP)

En 2013, la Agencia organizó el curso de verano «Retos de la protección de datos» en la sede de la Universidad Internacional Menéndez Pelayo, en Santander, que se celebró del 1 al 5 de julio y en el que se abordaron los múltiples retos que las nuevas tecnologías y los servicios de internet plantean en relación con la protección de datos. Se examinaron además las propuestas contenidas en la nueva normativa europea actualmente en tramitación con el fin de valorar su idoneidad para dar respuestas adecuadas a las demandas de la ciudadanía. El curso contó con la participación de directivos de la

Agencia, representantes de la Setsi, Inteco, Autocontrol, Apep, el Parlamento Europeo y la Comisión Europea.

- **Jornada de estudios sobre el nuevo marco europeo de protección de datos personales**

La AEPD organizó en colaboración con la Asociación Española para el Estudio del Derecho Europeo la Jornada de estudios sobre el nuevo marco europeo de protección de datos personales, celebrada el 20 de noviembre de 2013 en la Sala de Conferencias de la Representación en España de la Comisión Europea y del Parlamento Europeo.

Junto a estas acciones, la Agencia ha promovido diferentes **actividades de formación y documentación** con el objeto de contribuir al conocimiento especializado de la protección de datos personales y a la puesta a disposición de fondos documentales sobre esta materia a las personas interesadas.

En el primer aspecto, la AEPD ha mantenido una relación activa con diversas universidades públicas y privadas que ha permitido, mediante la celebración de convenios de colaboración, la realización de prácticas especializadas de estudiantes procedentes de las universidades de Alcalá de Henares, Carlos III, Autónoma de Madrid y Pontificia de Comillas. A ellos hay que añadir la visita investigadores de varias universidades latinoamericanas.

En el segundo, la Agencia continúa impulsando la creación de un fondo documental sobre protección de datos personales que, en el año al que hace referencia esta Memoria, se ha incrementado con la incorporación del fondo bibliográfico del Centro de documentación Pablo Lucas Murillo de la Cueva, procedente de la extinta Agencia de Protección de Datos de la Comunidad de Madrid.

2 GARANTIZAR LOS DERECHOS DE LOS CIUDADANOS

A - HERRAMIENTAS PARA FACILITAR EL CUMPLIMIENTO DE LA LOPD

Uno de los indicadores utilizados habitualmente para evaluar el nivel de conocimiento de la LOPD ha sido la inscripción de ficheros en el Registro General de Protección de Datos (RGPD).

El año 2013 finalizó con un total de 3.375.059 **ficheros inscritos** en el RGPD, una cifra que supone un incremento de un 12,4% respecto al año anterior. De ellos, 3.228.777 ficheros son de titularidad privada (el 95,66%) y 146.282 de titularidad pública (el 4,33 %).

El 87% de notificaciones de inscripción fueron presentadas a través de internet y el 13% restante en formato papel. El uso de la firma electrónica en la presentación de notificaciones se incrementa año tras año, suponiendo ya un 37% del total, frente al 33% de 2012.

Los ficheros privados inscritos han experimentado un incremento del 12% que, aun siendo relevante, supone una atenuación del ritmo de crecimiento experimentado en los años inmediatamente posteriores a la implantación del sistema NOTA y la publicación del Reglamento de desarrollo de la LOPD. Por su parte, el número de entidades responsables

<Índice>

de ficheros inscritos aumentó en un 11%, lo que pone de manifiesto el creciente conocimiento de la normativa de protección de datos en el sector empresarial español.

En lo que respecta a la finalidad de los ficheros de titularidad privada, los mayores incrementos porcentuales se han producido en los ficheros cuya finalidad es el *«Comercio electrónico»,* con un incremento de más del 25%, seguido de los que declaran tener por finalidad *«Guías/repertorios de servicios de comunicaciones electrónicas»* y *«Videovigilancia»,* con más de un 20%. La finalidad de *«Gestión de clientes, contable, fiscal y administrativa»* continúa siendo la más significativa, alcanzando el 59% de los ficheros inscritos. Los que sirven a otras finalidades, aunque registran incrementos significativos en los últimos años, todavía están lejos de ese porcentaje, como los ficheros de «*Videovigilancia»*, que suponen un poco más del 5% del total de inscritos.

Por sectores de actividad, los ficheros correspondientes al «*Comercio y servicios electrónicos*» han sufrido un incremento de más de un 23% y los de *«Actividades relacionadas con los juegos de azar y apuestas»* de casi un 20%.En términos absolutos, el mayor número de ficheros inscritos corresponde a las «*Comunidades de propietarios*» y a los sectores de *«Comercio», «Sanidad», «Turismo y hostelería» y «Contabilidad, auditoría y asesoría fiscal».*

El incremento de ficheros de titularidad pública durante 2013 fue del 6,5%. Hay que destacar el esfuerzo realizado por las corporaciones locales para adecuarse a la LOPD, que en 2013 han sido responsables de más del 82% del total de notificaciones realizadas.

En la Administración General del Estado (AGE), el Ministerio de Defensa destaca en cuanto a la inscripción de ficheros, habiendo incrementado su número en más de 500, lo que supone un aumento de más de un 44%.

Con respecto a las Administraciones de las Comunidades Autónomas hay que señalar en primer lugar la reorganización que están llevando a cabo y que tiene como consecuencia que, aunque se ha producido el alta de 752 ficheros, el número total ha disminuido en más de 1.100. Así, las Comunidades Autónomas de Aragón y Murcia han incrementado su número de ficheros inscritos en un 13% y un 10% respectivamente y, sin embargo, las Comunidades Autónomas de La Rioja y Madrid han disminuido su número total de ficheros inscritos en un más de un 15% y un 12% respectivamente como consecuencia de los procesos de reforma de estas Administraciones.

Destaca el caso de la Comunidad de Madrid, afectada por la desaparición de la Agencia de Protección de Datos de la Comunidad de Madrid con fecha 31 de diciembre de 2012, y que ha supuesto más de 10.000 operaciones de reorganización de ficheros inscritos en el RGPD.

En la Administración Local debe destacarse el esfuerzo de puesta al día que ha liderado la Diputación de Badajoz, y que ha producido que el número de ficheros inscritos de esta provincia se haya incrementado en más de un 220%. Con un incremento de casi un 200% se encuentra también la Administración Local de la provincia de Valladolid, que ha registrado un aumento de los responsables de ficheros, es decir, los Ayuntamientos, de un 79%, pasando de 105 a 188.

Los sujetos obligados al cumplimiento de la LOPD tienen disponible en la página web de la Agencia, entre otras **utilidades**, una *Guía del Responsable*, dirigida a conocer todas las obligaciones que le exi-

ge la LOPD; la herramienta DISPONE, para elaborar la disposición general de regulación de los ficheros públicos; una *Guía de Seguridad*, que permite conocer las medidas que tienen que implementarse para garantizar la seguridad de los datos personales sobre los que se llevan a cabo tratamientos;un Documento-guía editable, que permite elaborar el documento de seguridad; la herramienta EVALÚA, que permite realizar un autodiagnóstico a través de la contestación a un test de preguntas para conocer el nivel de cumplimiento de la LOPD o el nivel de implementación de las medidas de seguridad; así como los procedimientos electrónicos que permiten enviar las notificaciones de ficheros mediante el formulario NOTA, solicitar información sobre los ficheros inscritos o consultar el estado de tramitación de las solicitudes.

A estas utilidades hay que sumar otro **catálogo de guías** dirigidas a facilitar información sobre el cumplimento de obligaciones en relación con materias concretas, como la *Guía de Videovigilancia*, la Guía *La protección de datos en las relaciones laborales*, la *Guía sobre el uso de las cookies*, la *Guía para clientes que contraten servicios de Cloud computing*, las *Orientaciones para prestadores de servicios de Cloud Computing*, la *Guía de Seguridad de Datos*, la *Guía sobre seguridad y privacidad*

<Índice>

de las tecnologías RFID, y la *Guía del responsable de ficheros*.

Los siguientes datos muestran la acogida de estos servicios en el ejercicio 2013:

- El formulario NOTA ha tenido 415.963 accesos para notificar ficheros a la Agencia.
- Se han solicitado 14.915 copias de contenido de ficheros.
- 10.589 usuarios han realizado el test EVALÚA LOPD.
- 3.554 usuarios han realizado el test EVALÚA SEGURIDAD.
- Se ha accedido en 4.828 ocasiones a la herramienta DISPONE, que permite preparar la disposición general de regulación de ficheros públicos.
- La *Guía de seguridad* ha sido consultada y/o descargada en 52.005 ocasiones.
- El modelo de documento de seguridad ha sido descargado en 91.771 ocasiones.
- El resto de guías dirigidas a responsables del tratamiento han tenido el siguiente número de descargas:
  - *Guía del responsable de ficheros*: 181.255
  - *Guía de videovigilancia*: 91.469
  - Guía *La protección de datos en las relaciones laborales*: 337.238
  - *Guía para clientes que contraten servicios de Cloud computing*:228.159
  - *Orientaciones para prestadores de servicios de Cloud computing*: 87.660
  - *Guía sobre el uso de las cookies*: 218.968
  - *Guía sobre seguridad y privacidad de las tecnologías RFID*: 140.354

Por otra parte, con el fin de facilitar el cumplimiento de la LOPD en sectores específicos, la Agencia ha continuado desarrollando la labor de orientación a los promotores de **códigos tipo** interesados en promover estos instrumentos de autorregulación en su sector de actividad.

Dentro de esta actividad de orientación previa hay que mencionar el proyecto de código tipo para las oficinas de Barcelona promovido por el Colegio Oficial de Farmacéuticos de dicha ciudad, que se ha llevado a cabo en cooperación con la Autoridad Catalana de Protección de Datos atendiendo a que el ámbito objetivo del código tipo alcanza a tratamiento y ficheros de su competencia.

Con la misma finalidad han continuado las reuniones con la Federación Nacional de Clínicas Privadas (FNCP), la Asociación Nacional de Actividades Médicas y Odontológicas de la Sanidad Privada (AMOSP) promotoras de un código tipo al que también se han incorporado la Asociación Catalana d'Entitats de Salut (ACES) y la Asociación de Empresas Sanitarias de Prestación Asistencial de Andalucía (AESPAA). Ambos proyectos podrían estar finalizados para su aprobación en 2014.

Estas iniciativas consolidan la tendencia del interés específico de las entidades del sector sanitario para promover instrumentos de autorregulación que adapten las garantías de la normativa de protección de datos a la complejidad y especificaciones del tratamiento de los datos de salud.

También se han mantenido reuniones con representantes de la Asociación Empresarial de Gestión Inmobiliaria (AEGI) con vistas a modificar el código tipo del sector de la intermediación inmobiliaria, inscrito en el Registro General de Protección de Datos, así como con la Asociación Nacional de Entidades de Gestión del Cobro (ANGECO), como promotora de un código de conducta para un sector que habitualmente trata datos de carácter personal en el desarrollo de su actividad.

Por último, en cumplimiento de las obligaciones posteriores a la inscripción del código tipo establecidas en el artículo 78 b) del RLOPD, durante 2013 se han recibido de los promotores de los códigos tipo inscritos en el RGPD las memorias anuales correspondientes a la actividad del 2012 y se ha requerido la de aquellos otros promotores que no la habían enviado.

En cuanto a las **consultas** de mayor complejidad dirigidas a facilitar la aplicación de la LOPD a los responsables de tratamientos públicos y privados, se atendieron un total de 489, de las cuales 318 (65%) fueron planteadas por las Administraciones Públicas y 171 (35%) por el sector privado.

Se mantiene, por tanto, en una cifra similar el volumen de consultas planteadas respecto a las formuladas el año anterior, aun cuando tales cifras implican una reducción frente a las de los años inmediatamente posteriores a la entrada en vigor del RLOPD y, en particular, a los años 2008 a 2009. Ello puede ser debido a la mitigación del efecto producido como consecuencia de esa entrada en vigor, que hizo incrementarse en gran medida el número de consultas. Del mismo modo, cabe apreciar que en 2013 se ha producido una mayor singularidad en el contenido de las consultas planteadas, así como una reducción de las dudas de carácter general que habían podido suscitarse tras la entrada en vigor del Reglamento, y que fueron resueltas en los informes emitidos a consultas planteadas en los dos ejercicios anteriores.

Igualmente se aprecia, en cuanto al reparto de las consultas de los sectores público y privado, la cada vez mayor preponderancia de las procedentes del sector público (en este ejercicio ya alcanzan el 65% del total, incrementándose un 9% en términos absolutos).

El análisis de las cuestiones planteadas permite extraer las siguientes conclusiones sobre la evolución de las consultas en el año 2013:

- El mantenimiento del número relativamente significativo de consultas relacionadas con la aplicación de la regla de ponderación de derechos e intereses contenida en el artículo 7 f) de la Directiva 95/46/CE, que en 2013 ascendieron a 15 (un incremento del 7% respecto al ejercicio anterior).

- El notable crecimiento 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 en los tratamientos, produciéndose un incremento del 74% y suponiendo un 23% de las consultas las que han exigido analizar esta cuestión. También es relevante el incremento en un 44% de las consultas relacionadas con ficheros de titularidad pública.

- El incremento de las consultas relacionadas con el tratamiento de datos de salud, que ascienden en un 17% respecto del ejercicio anterior.

- El mantenimiento de un número relevante de cuestiones relacionadas con las cesiones

de datos (manteniendo un volumen superior al 40%), siendo igualmente relevante el número de cuestiones relacionadas con los requisitos para la prestación del consentimiento (un 20% del total).

- El moderado descenso de las cuestiones relacionadas con el ámbito de aplicación de la normativa de protección de datos, el ejercicio de derechos y las medidas de seguridad.

- El muy notable descenso de las consultas relacionadas con las obligaciones del encargado del tratamiento (un 72%) y las transferencias internacionales de datos (de un 90%, frente al incremento del 500% que habían sufrido en 2012).

Atendiendo a la distribución sectorial de las consultas del sector privado, las principales conclusiones son:

- La práctica desaparición de las consultas procedentes de entidades dedicadas a la asesoría y consultoría, dado que, transcurridos más de cinco años desde la entrada en vigor del Reglamento, la Agencia mantiene el criterio general de atender únicamente las consultas relacionadas con sus ficheros y tratamientos y no con las de sus clientes, que deben ser formuladas por estos últimos. Estas consultas representan ya sólo un 2% del total y un 5% de las procedentes del sector privado.

- El mantenimiento de las consultas planteadas por particulares, que ya son las más abundantes dentro del sector privado.

- El incremento notable de las consultas procedentes de sindicatos y partidos políticos, que se cifra en un 260%. Igualmente, es notable el número de consultas procedentes de las empresas de suministro de agua, gas y electricidad, que pasan de 1 a 8 en este ejercicio.

- El mantenimiento de las consultas procedentes de asociaciones no profesionales y fundaciones, que en 2012 habían sufrido un importante descenso.

- El moderado descenso de las consultas procedentes del sector de las telecomunicaciones, que descienden un 31% respecto del ejercicio anterior.

- El notable descenso de las consultas procedentes del denominado tercer sector, que se reducen en un 57%, así como el de las empresas de servicios informáticos (que disminuyen en un 67%).

- En el sector público se reduce el peso de las consultas formuladas por la Administración General del Estado, que desciende del 66% al 52%, disminuyendo asimismo un 15% en términos absolutos, frente al aumento en un 71% de las consultas procedentes de las Comunidades Autónomas, en buena medida como consecuencia de la asunción por la Agencia Española de Protección de Datos de las competencias de la extinta Agencia de Protección de Datos de la Comunidad de Madrid.

Los informes no preceptivos relacionados con consultas externas que pueden revestir una mayor trascendencia en materia de protección de datos versaron, entre otras, sobre las siguientes materias:

- Los requisitos para la creación por diversas entidades de sistemas de prevención del fraude de carácter sectorial, a fin de poder considerar el tratamiento de los datos fundado en el artículo 7 f) de la Directiva 95/46/CE.

- Diversas cuestiones relacionadas con la aportación de información genética de personas fallecidas a la base de datos creada por el Instituto Nacional de Toxicología y Ciencias Forenses en relación con la investigación de los supuestos de sustracción de niños recién nacidos, así como los requisitos para la actuación en estos procedimientos de las asociaciones representativas de los colectivos afectados.

- La procedencia del intercambio de información entre los Ministerios de Justicia e Interior para la asistencia a las víctimas del terrorismo.

- La licitud del tratamiento de los datos de ideología política de concejales electos, al haberse hecho manifiestamente públicos por aquellos, así como la aplicación a los ficheros que sólo contengan este dato de las medidas de seguridad de nivel básico y no alto.

- La procedencia del acceso por el Instituto Nacional de Estadística a los datos relacionados con las altas y bajas de contratos de telefonía móvil, dada la incidencia que puede revestir en la encuesta de migraciones, si bien únicamente como experiencia piloto, debiendo acreditarse su utilidad al término de tal programa.

- La improcedencia del uso por un fabricante de vehículos de los datos del Registro de vehículos con finalidad de publicidad.

- La aclaración del modo en que debe interpretarse la exigencia de medidas de seguridad de nivel alto en los ficheros relacionados con el cumplimiento de la legislación de prevención del blanqueo de capitales, exigiéndose dicho nivel únicamente para los ficheros relacionados con el examen especial de operaciones y la comunicación por indicio al SEPBLAC.

- La delimitación del alcance de la información a facilitar en aplicación de las normas que han venido a modificar el régimen de retribución de los empleados públicos en situación de incapacidad temporal, que no exige especificar más que la concurrencia de una de las circunstancias que determinan la no detracción de los haberes.

- Los requisitos para que una entidad financiera pueda hacer uso de la información que figura en los recibos domiciliados para el abono de la prima de un determinado seguro con la finalidad de ofrecer los seguros que comercializa a través de sus acuerdos.

- La licitud de la reproducción por una televisión autonómica de imágenes recogidas por cámaras que captan panorámicas de distintos emplazamientos urbanos de varias ciudades, en las que las imágenes relacionadas con personas concretas aparecen de forma meramente accesoria y grabadas a una gran distancia, lo que las hace difícilmente reconocibles.

- La necesidad de información a los empleados para que sea posible la utilización por el empresario de las imágenes captadas por dispositivos de videovigilancia para el control de la relación laboral, siguiendo la doctrina del TC en su sentencia 29/2013.

- El sometimiento a la normativa de protección de datos de los sistemas de videovigilancia en la zona de acceso a centros penitenciarios.

- La improcedencia de que una Administración a la que otra solicita datos de un interesado para su aportación a un determinado expediente, constando el consentimiento de aquél, pueda oponerse a la remisión de dicha información

por considerarla innecesaria en el ámbito del citado expediente.

- Los requisitos de proporcionalidad y seguridad que deberán cumplirse para que sea posible la inclusión de información personal de cualquier paciente en una pequeña medalla colgada del cuello en el que se pueda visualizar un Código QR con fines sanitarios, incluyendo la historia clínica del paciente.

- La posibilidad de que una Administración Pública pueda otorgar a un órgano determinado la gestión de sus sistemas de información, ostentando así la condición de encargado del tratamiento, si al delimitarse sus competencias se han especificado las obligaciones derivadas de lo dispuesto en la LOPD.

- La determinación de los requisitos que habrá de reunir el requerimiento de pago previo a la inclusión de los datos en los ficheros de solvencia patrimonial y crédito. En particular, poniendo de relieve que no es ajustado a la LOPD realizar dicho requerimiento a través de llamadas telefónicas automatizadas a números fijos y/o móviles registrados en el contrato del que deriva la deuda.

- El carácter excesivo del establecimiento de un sistema que pretendía la cesión por los operadores de telecomunicaciones a los servicios de emergencia del dato de localización del usuario a fin de avisar a este de alertas de grandes emergencias.

- La necesidad de obtener el consentimiento de los empleados públicos para poder captar imágenes de los mismos en oficinas públicas.

- Los requisitos exigibles para que sea posible la captación, conservación o difusión de imágenes de alumnos de un centro educativo por el propio centro.

- Diversas cuestiones relacionadas con la licitud de la difusión en redes sociales de información de menores, trabajadores (dentro de un perfil corporativo) o intervinientes en eventos organizados por el titular del perfil (en este caso un sindicato, lo que podría revelar datos de ideología o afiliación sindical).

- La legitimación de los titulares de la patria potestad para acceder a historias clínicas de menores salvo que por ley se establezca lo contrario en supuestos concretos.

B - UNA RESPUESTA INTEGRAL A LAS NECESIDADES DE LOS CIUDADANOS

El año 2013 ha supuesto la consolidación en el número de reclamaciones planteadas por los ciudadanos ante la Agencia.

En 2010 las denuncias y reclamaciones de tutela de derechos presentadas ante la Agencia ascendieron a 6.702, en 2011 crecieron hasta alcanzar las 9.878 y en 2012 se situaron en 10.787. En el año 2013 se ha consolidado el número global, aunque con un ligero descenso del 1,70% motivado por una disminución del 8,94% en el número de escritos de reclamación de tutela presentados. Por el contrario las denuncias han crecido un 0,15%.

El número de resoluciones dictadas por la Agencia ascendió a 7.856 en 2011, una cifra que se elevó a 10.995 en 2012, con un incremento en un año de casi el 40%. En 2013, se ha mantenido este elevado volumen de resoluciones con un ligero descenso del 2,31% (10.741).

Destaca el hecho de que las resoluciones de procedimientos sancionadores se han visto incrementadas en un 11,30%. Y, en paralelo, se ha producido un aumento de las resoluciones de archivo en un 4,29% frente a las declarativas de infracción que disminuyen en un 2,46%.

Las principales razones que han motivado este alto número de archivos –bien como consecuencia de las inadmisiones a trámite (que aumentan un 7,53%) o de archivo tras actuaciones de investigación (que disminuyen en un 5,72%)– son sustancialmente las mismas que se han descrito en memorias de años anteriores:

a) Inaplicación de la LOPD que puede producirse por diversas razones:

– Por estar el asunto excluido de su ámbito territorial de aplicación.

– Por ser el denunciante o el afectado una persona jurídica.

– Por realizarse tratamiento de datos relativos a fallecidos no amparados por la LOPD.

– Por suscitarse cuestiones que están fuera del ámbito competencial de la AEPD tales como la facturación o el consumo, deficiencias en la prestación del servicio, interpretación sobre cláusulas contractuales o envío de mensajes de tarificación adicional Premium.

b) Aplicación de las garantías del procedimiento sancionador, que se traduce en la necesidad de acordar la inadmisión o el archivo por inexistencia de indicios razonables para abrir una investigación.

c) Prevalencia de otros derechos o intereses legítimos como la tutela judicial efectiva, la libertad sindical o la libertad de expresión e información.

d) El carácter excepcional del procedimiento sancionador si el ordenamiento permite otras fórmulas como el ejercicio de derechos de acceso, rectificación, cancelación y oposición.

e) La falta de competencia de la Agencia por razones de territorialidad, como los casos relativos a directorios de internet que reproducen guías telefónicas desactualizadas. En estos casos, la LOPD no resulta aplicable al no tener sus responsables establecimiento en España desde el que se realicen tratamientos asociados a los servicios que prestan ni utilizar medios en España.

Las resoluciones de procedimientos de apercibimiento han recaído mayoritariamente en la actividad de videovigilancia (59,82%) debido a que frecuentemente los denunciados son particulares y pymes, ámbito en el que procede aplicar los criterios de disminución de culpabilidad y antijuridicidad exigidos en la LOPD así como el requisito de no haber sido sancionados o apercibidos previamente. A gran distancia se encuentran los servicios de internet (8,68%) que, sin embargo, crecen un 11,76% respecto a 2012.

El volumen de las sanciones económicas declaradas creció en 2013 un 6,10%, alcanzando la cifra de 22.339.440 euros.

En relación con las sanciones, cabe destacar que en casi el 84% de los casos (83,77%) se han aplicado los criterios de moderación y atenuación previstos en los apartados 4, 5 y 6 del artículo 45 de la LOPD. Asimismo, debe tenerse en cuenta que en un solo procedimiento se declararon tres infracciones, imponiéndose una sanción de 900.000 euros.

Manteniendo la tendencia de años anteriores, el sector de actividad en el que se ha declarado un mayor volumen de sanciones ha sido el de las te-

lecomunicaciones en el que, aunque desciende levemente (-2,17%) respecto del año anterior, ha alcanzado un importe total de 15.035.008 euros. Descenso que se produce pese a constatarse un incremento de las resoluciones declarativas de infracción del 9,69% en este sector.

Resulta relevante señalar que el sector de suministro y comercialización de agua y energía ha pasado a ocupar el segundo lugar en cuanto a volumen de sanciones con un importe de 2.084.901 euros, superando al relacionado con la actividad de las entidades financieras. Este volumen global de sanciones debe ser matizado, no obstante, por el hecho de que una sola empresa del sector de la energía ha sido sancionada con 1.250.001 euros. Las resoluciones declarativas de infracción en los sectores citados se incrementaron en un 65,52%.

Asimismo, se ha producido un importante incremento de resoluciones sancionadoras respecto de las comunicaciones comerciales electrónicas (51,28%) y otros servicios de internet (12.82%).

Las resoluciones más reseñables sobre responsables privados (con excepción del procedimiento a un prestador de servicios de internet sancionado con 900.000 euros -PS/00345/2013-, que se recoge en otro apartado de la Memoria) se detallan a continuación:

- **Tratamiento de datos en internet:**
  - Campaña de recogida de datos para el servicio Google Street View (E/01829/2012)

La Agencia Española de Protección de Datos concluyó la investigación sobre la última campaña llevada a cabo por Google para actualizar su servicio Street View. En ella constató que no se recogen datos transmitidos por redes inalámbricas sino únicamente imágenes fotográficas. La Agencia concluyó que la campaña de recogida de imágenes y su posterior tratamiento para la prestación del servicio no vulnera la normativa española de protección de datos.

La AEPD aplicó la doctrina establecida por el Tribunal de Justicia de la Unión Europea en su sentencia del 24 de noviembre de 2011 según la cual, a pesar de que el tratamiento de datos de carácter personal requiere el consentimiento del afectado, éste no será preciso cuando el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable *«siempre que no prevalezcan los derechos y libertades fundamentales del interesado».*

La Agencia realizó una ponderación entre el interés legítimo y la captación de imágenes de calles y carreteras para la prestación del servicio Street View, y el grado de afectación de los derechos de los afectados por estas actividades.

A estos efectos, valoró que *«la finalidad de Google Street View no es obtener información relativa a las personas, cuya recogida es incidental. Tampoco lo es la identificación de los afectados, ni el tratamiento posterior para su divulgación. La finalidad última de la recogida de información llevada a cabo es la prestación de un servicio de cartografía».*

Asimismo, tuvo en cuenta que las imágenes en las que aparecen personas o vehículos son sometidas antes de su publicación a un proceso de anonimización consistente en difuminar, de manera permanente e irreversible, los rostros y matrículas para que no puedan ser reconocidos; que los programas diseñados para la recogida y procesamiento de imágenes no disponen de instrumentos de reconocimiento facial ni permiten la búsqueda por personas; que las imágenes que se ofrecen son estáticas y no identifican la fecha de su captación; y

que sólo se conservan las fotografías originales por el período necesario para la mejora del servicio o el cumplimiento de los fines para los que fueron recabados los datos personales.

Se concedió especial relevancia al compromiso de Google de mantener un mecanismo que permite al usuario solicitar la corrección de los eventuales errores que se produjeran en este proceso de anonimización, permitiendo así ejercitar el derecho de cancelación previsto en el artículo 16 de la LOPD. En caso de no ser atendido, los usuarios pueden dirigirse a la AEPD para solicitar la tutela de sus derechos.

Esta resolución de archivo de actuaciones es una actuación independiente del procedimiento sancionador que la AEPD abrió a Google por la captación de datos personales procedentes de redes WiFi. En este último caso, la AEPD constató la existencia de indicios de la comisión de cinco infracciones -dos graves y tres muy graves- de la LOPD, iniciándose un procedimiento sancionador que se encuentra suspendido ante la existencia de un procedimiento judicial penal pendiente.

- Suplantación de identidad (PS/00197/2013, PS/00595/2012)

Se denunció la creación de un perfil fraudulento en una red social en la que se publica una fotografía de la persona afectada asociada a su nombre de pila, edad, ubicación y número de teléfono.

A partir de la información facilitada se logró determinar que el perfil fue creado y actualizado a través de conexiones vinculadas a una línea de la que era titular la sancionada.

- Publicidad de sentencias sin anonimizar en página web (A/00225/2012)

En la web de la asociación denunciada se incorporó sin anonimizar una sentencia en la que constan los datos de los miembros de la Guardia Civil denunciantes (nombre, apellidos, escala, destino).

La asociación actuó en el ejercicio de los fines y actividades que le son propios al tratarse de una sentencia de interés para el colectivo, aunque lo divulga a terceros, razón por la que se apercibió.

- Identidad de personas presuntamente implicadas en caso de torturas (PS/00366/2012)

Se denuncia que desde distintas páginas web son difundidos datos personales relacionados con casos de torturas. La información no resulta veraz, al difundir una noticia sobre unas sentencias en las que el denunciante no aparece como condenado ni imputado, por lo que no puede prevalecer el derecho constitucional a la libertad de información. Tampoco puede invocarse el principio de publicidad de las resoluciones judiciales o la existencia de un interés legítimo. El hecho de que se trate de una noticia recogida en internet no avala dicho tratamiento de datos, pues no se está ante una fuente de acceso público.

- Imágenes de menores grabadas con cámara oculta (PS/00733/2012)

La denunciante, madre separada, cuando va a buscar a sus hijos al colegio observa como un tercero quiere recogerles por encargo del ex marido con una cámara oculta que graba los hechos para luego colgarlos en internet.

Posteriormente, se emiten en YouTube y en la web de la entidad denunciada (una asociación de padres separados) imágenes captadas con la cámara

oculta. En el vídeo se visualiza a dos menores y a la madre.

- **Videovigilancia**

En 2013 se han dictado variadas resoluciones centradas en las infracciones más habituales en el ámbito de videovigilancia:

- Captación de la vía pública que, como regla general, se reserva a las Fuerzas y Cuerpos de Seguridad

En relación con este tipo de infracción, pueden reseñarse, entre otras muchas, dos resoluciones de Apercibimiento (A/00160/2013 y A/00125/2013), recaídas respectivamente contra una sociedad cultural recreativa, y contra una sociedad rectora bursátil. En ambos casos, algunas de las cámaras instaladas se encontraban orientadas hacia la calle, captando imágenes desproporcionadas y enfocando directamente a la acera y a la calzada de la vía pública.

Asimismo, la Agencia ha dictado varias resoluciones sancionadoras en el marco de los correspondientes procedimientos instruidos en materia de videovigilancia con ocasión de la captación y/o grabación de imágenes de la vía pública. A modo de ejemplo, se pueden mencionar los procedimientos PS/00255/2013, seguido contra una entidad bancaria, y PS/00300/2013, incoado contra una cadena hotelera, ambos relacionados con la instalación de cámaras a través de las cuales se procedía al visionado y/o grabación de imágenes en la vía pública.

- Ausencia de cartel informativo

Las resoluciones de Apercibimiento dictadas en el marco de los expedientes A/00034/2013 y A/00085/2013 fueron realizadas como consecuencia del incumplimiento del deber de información, al verificarse la ausencia de carteles en los que se avisara de la presencia de las cámaras y en los que se recogiese la identidad de la persona responsable de las mismas ante quien ejercitar los derechos de acceso, rectificación, cancelación y oposición previstos en la LOPD.

- Captación proporcionada de imágenes (E/07192/2012)

Archivo de una denuncia centrada en la divulgación de un vídeo sobre hechos sucedidos en la puerta de un Ayuntamiento donde se produjo una protesta y realizado con imágenes de la cámara de seguridad del propio Ayuntamiento.

Según se observó mediante el visionado de las imágenes captadas por dicha cámara, la utilización del sistema de cámaras para la obtención de imágenes resultaba proporcional en relación con el fin perseguido: la vigilancia, control de accesos y seguridad de los diferentes locales y dependencias municipales y sus alrededores; seguridad y control de acceso a edificios.

- **Alta en la contratación de servicios sin consentimiento**

En 2013 se han presentado numerosas denuncias que han derivado frecuentemente en la imposición de sanciones por la realización de altas de contratos sin consentimiento.

Tal circunstancia ha sido especialmente relevante en el ámbito de la energía en supuestos en los que la entidad no acredita en forma alguna el consentimiento de la persona afectada, cuyos datos habitualmente han sido recabados a través de una empresa comercializadora (PS/00282/2013, PS/00370/2013 y PS/00410/2013). La responsabilidad en estos supuestos es concurrente entre

el encargado de tratamiento y el responsable al no recabar, poder aportar ni controlar en el caso del responsable documentación acreditativa de haber adoptado la diligencia necesaria. A mayor abundamiento, a pesar de no disponer de la acreditación del consentimiento, el responsable ha seguido reclamando la deuda y en ocasiones ha incluido los datos del afectado en ficheros de solvencia.

Entre los supuestos que han derivado, en sentido contrario, en archivos de la denuncia se encuentran aquellos en los que el denunciante, tras otorgar su consentimiento, cambió de parecer. Así, en el E/03225/2012, una persona que solicitó la portabilidad se retractó posteriormente, recibiendo facturas relativas a dichas líneas por incumplimiento del compromiso de permanencia y siendo sus datos incluidos en ficheros de morosidad sobre los que no corresponde a la Agencia –una vez comprobada la existencia de consentimiento– dilucidar la procedencia o no de la deuda generada.

Inclusión en ficheros de información sobre solvencia patrimonial

La inclusión en ficheros de solvencia también ha sido objeto de múltiples resoluciones que verifican el cumplimiento de los aspectos en los que resulta competente la Agencia:

- La omisión del requerimiento previo a la inclusión en el fichero (PS/00010/2013, PS/00015/2013 y PS/00035/2013).
- El incumplimiento del principio de calidad de los datos según el cual, cuando el deudor ha presentado una reclamación ante una instancia judicial, arbitral o administrativa competente para resolver sobre la certeza de la deuda, los datos personales no podrán incluirse o mantenerse en los ficheros de esta naturaleza (PS/00002/2013, PS/00004/2013, PS/00005/2013 y PS/00012/2013).
- La falta de cancelación inmediata, tras el pago de la deuda, del dato relativo a la misma (PS/00011/2013, PS/00014/2013 y PS/00043/2013).
- La consulta de los datos de una persona sin legitimación para ello (PS/00199/2013 y PS/00386/2013).
- La inclusión de un DNI vinculado a datos de otra persona (PS/00007/2013, PS/00036/2013 y PS/0200373/2013).

En línea con esta última resolución debe subrayarse que la condición de moroso no puede resultar de público conocimiento sino que el acceso se debe limitar a aquellas personas afectadas o interesadas por tal condición definidas –para el caso de ficheros de solvencia– en el artículo 42 del Reglamento de la LOPD. Este principio resulta aplicable también en una comunidad de vecinos en los que estos tienen derecho como interesados a conocer la identidad del moroso, sin que la misma pueda hacerse pública a terceros. Así, el PS/00280/2013 sancionó la exposición de una lista de morosos en un tablón situado en la vía pública.

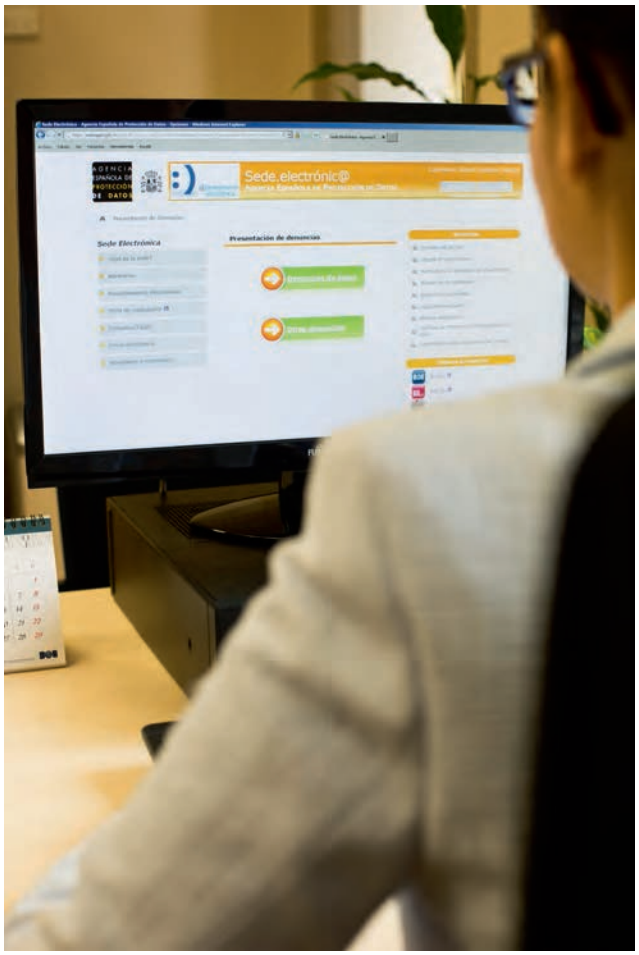
Publicidad

En el año 2013 se ha continuado recibiendo denuncias sobre comunicaciones publicitarias tanto a través del canal telefónico como de servicios de la sociedad de la información.

En relación con el envío y recepción de comunicaciones comerciales se aprecia que, junto a la presentación de denuncias por incumplimiento de las

normas que lo regulan, continúa creciendo el número de ciudadanos que desarrollan una conducta activa para limitar la publicidad que reciben utilizando la opción de registrarse en la Lista Robinson, gestionada por Adigital.

Así, el número de usuarios registrados en la Lista Robinson ascendió a 347.012 en 2013, de los que el 19,31% optaron por restringir la publicidad a través de correo postal, el 19,89% por correo electrónico y el 20,14% mediante sistemas de comunicación electrónica (SMS/MMS).



La reacción de los ciudadanos que quieren limitar las comunicaciones publicitarias alcanza su mayor nivel de intensidad en el canal telefónico en el que, con 247.927 inscritos, figuran registrados el 40,66% de los usuarios de la lista Robinson.

- Llamadas telefónicas comerciales (PS/00682/2013, PS/00231/2013 y PS/00232/2013)

Se sancionó a una operadora de telefonía porque sus distribuidores realizaron llamadas comerciales a personas que tenían registrada su línea telefónica en el servicio de Lista Robinson.

La denunciada reconoció la culpabilidad, pero al existir numerosas denuncias por hechos similares, no procedía aplicar los criterios moduladores de la sanción.

Frente a estos hechos, en supuestos como el E/00001/2013, tras las actuaciones previas de investigación no pudo acreditarse que el denunciante recibiera llamadas procedentes de la misma operadora en los días y horas indicados en el escrito de denuncia.

- Publicidad a través de correo electrónico (PS/00435/2013, PS/00400/2013 y PS/462/2013)

En estos expedientes los denunciantes recibieron correos electrónicos publicitarios tras haber solicitado la baja en el servicio, o sin su consentimiento, procedimientos que finalizaron con imposición de sanción.

Por el contrario, en el E/5608/2013 se denunció la remisión de correos publicitarios sin consentimiento, pero se archivó por la existencia de una relación contractual previa.

<Índice>

- Publicidad viral (A/00112/2013)

El denunciante recibió un correo electrónico en el que se le invitó a que aportara los datos personales de sus contactos a cambio de una participación de lotería. El remitente del envío era una persona jurídica de la que fue cliente.

Se estimó que concurría un tratamiento de datos sin consentimiento —al desviarse de la finalidad para la que inicialmente fueron captados— en dos aspectos. Respecto del cliente, porque el tratamiento de datos cuya legitimación ostentaba la empresa era para prestarle el servicio, no para utilizarlo como medio de captación de potenciales clientes a cambio de un beneficio (en este caso, un décimo de lotería). En la factura aportada que acredita que el denunciante compró un producto a la empresa no se especifica dicho fin respecto del tratamiento de sus datos. En el segundo, respecto de la entidad que se nutre de una base de datos para enviarles publicidad a través de personas como el cliente, porque no tiene el consentimiento de estas personas para recabar sus datos.

- Publicidad viral a través de una red social (PS/00663/2012)

Usuarios de una red social reciben comunicación de otros usuarios informándoles de que salen en un vídeo, proporcionando un link. Al pulsar sobre él se pide la confirmación para descargar un software como complemento para la ejecución del vídeo. Al instalar este complemento, se solicita la introducción de un número de teléfono móvil para comprobar la edad a través de un código de confirmación, redirigiendo al navegante a un sitio web mientras se ejecuta un software para enviar, haciéndose pasar por el usuario de la red, la comunicación comercial a los muros de al menos 30 usuarios más, continuando el proceso de difusión viral.

El tratamiento sin consentimiento sucede cuando a través del software malicioso instalado por la empresa subcontratada de la campaña publicitaria se envía una comunicación comercial que se publica en el muro de los demás usuarios, haciendo creer que dicha información ha sido publicada por un usuario concreto. Acontece una suplantación de identidad, pues realmente dicha información no es subida a la red por el usuario.

- **Comunicación de datos a las Autoridades de Estados Unidos (E/06406/2012)**

En el marco del expediente se realizaron actuaciones de inspección ante tres compañías aéreas por la comunicación de datos de los pasajeros de dichos vuelos a las autoridades de Estados Unidos.

Las actuaciones concluyeron que las citadas compañías aéreas cumplían correctamente con el deber de información a sus clientes a la hora de adquirir un billete para vuelos que sobrevolasen Estados Unidos y que la comunicación de datos a las autoridades estadounidenses se amparaba en las disposiciones del Convenio sobre Aviación Civil Internacional, denominado Convenio de Chicago, suscrito por España el 7 de diciembre de 1944.

Respecto de las **Administraciones Públicas,** en 2013 se ha producido un importante incremento de un 52,63% en el número de resoluciones de procedimientos de infracción.

De ellas cabe destacar las siguientes:

■ Calidad de datos (AP/00039/2012)

Se declaró infracción por tratamiento de datos inexactos porque se atribuyó una deuda de la tasa de basuras y se emitió una diligencia de embargo de cuentas bancarias a una persona que no era el deudor.

■ Deber de secreto (AP/00034/2013)

Una Consejería entregó a la esposa del denunciante un certificado y la hoja de servicios en los que consta su vida laboral. La Consejería no recabó el consentimiento del denunciante para la entrega de dicho documento, que su esposa utilizó en un procedimiento de demanda de divorcio.

■ Medidas de seguridad (AP/00015/2013)

Varias personas denunciaron que una Gerencia de Salud remitió a sus domicilios una resolución en la que, junto a los datos personales del afectado, se reseñaba la referencia *«sanción consumo alcohol»*. Los datos contenidos en la *«nota informativa»* quedaban a la vista de cualquiera, siendo accesibles por terceras personas, al incluirse el aviso en la tarjeta de acuse de notificación, en el ejemplar de notificación de resolución de procedimiento sancionador y en una tarjeta completamente abierta, no introducida en ningún sobre ni con ningún tipo de envoltorio, que fue depositada por el cartero en su buzón.

Las notificaciones se enviaron de forma masiva y aunque no se acreditó el acceso por terceros —que hubiera supuesto una infracción por deber de secreto— derivó en la declaración de una infracción por incumplimiento de las medidas de seguridad exigibles.

■ Deber de información previo para acceder al correo corporativo de los trabajadores (AP/00031/2012)

Los directores de cada área de un organismo público tenían permisos para acceder al contenido del correo corporativo del personal de su área, en el cual se incluían las carpetas personales.

En la inspección se constató que no se proporcionó previamente al personal información sobre las reglas aplicables al control del correo electrónico ni sobre acceso por los directores de área. Se resolvió declarando la infracción por vulneración del deber de información.

■ Listados sobre la adscripción política de funcionarios (AP/00023/2013)

Un grupo municipal denunció que le había llegado de forma anónima una memoria USB que contenía un fichero en formato Excel con los datos personales y laborales de empleados del Ayuntamiento, con siglas de un partido político o el apellido del alcalde que gobernaba cuando el empleado entró en el ayuntamiento.

Se inició procedimiento por tratamiento de datos excesivos y por falta de medidas de seguridad.

Se archivaron las actuaciones al constatarse que la finalidad de los listados denunciados era el estudio estadístico de las contrataciones realizadas por cada gobierno municipal; que se había hecho una investigación por la filtración de este estudio y adoptándose nuevas medidas de seguridad además de las ya implantadas. Junto a ello se apreció que los datos personales no habían salido de la esfera del Ayuntamiento.

<Índice>

■ Análisis del aplicativo SIGO, que incorpora las identificaciones realizadas por agentes de la Guardia Civil (E/03654/2012)

Se denunció la inclusión y conservación en diversos ficheros del Ministerio del Interior a través de la aplicación SIGO de personas que carecían de antecedentes penales o policiales, y que no habían cometido infracciones administrativas.

El análisis de la información obtenida en las actuaciones previas de inspección permitió destacar los siguientes aspectos:

- Las identificaciones son selectivas y de interés policial, no realizándose de forma indiscriminada ni conforme a un cupo por agente.
- Los datos se recaban en función de la relevancia que le atribuye el agente en función del punto de identificación, sin que existan campos obligatorios ni un modelo común.
- El volumen de identificaciones es distinto en diversas comandancias, variando para un mismo puesto en distintas fechas y sin ser un porcentaje que dependa del número de efectivos destacados o de las patrullas realizadas.
- Del conjunto de personas identificadas se graban los datos de las que parecen más relevantes, almacenándose una de cada cuatro identificaciones.

Respecto a la proporcionalidad del volumen de información recogida, los resultados de la inspección realizada a los datos almacenados a través del sistema SIGO evidenciaron que el volumen de personas registradas como identificadas es un porcentaje limitado de la población. Además, en el caso de identificaciones, no se almacena toda la información que acepta el sistema en relación con ellas, ya que en las pantallas de SIGO aparecen muchos campos relativos a la identificación que no se rellenan si no se consideran relevantes. Asimismo, en la inspección se concluye que no se recoge información de todos los ciudadanos involucrados en la identificación, sino que esta se realiza de forma selectiva. Y, en muchos casos, no se registra información alguna de los ciudadanos identificados.

De ello se deduce que el criterio utilizado por la Guardia Civil en la recogida de datos no es el registro sistemático de toda la información que es posible recoger en una actuación de identificación.

En cuanto a los periodos de conservación de la información y el acceso a la misma, los resultados de la inspección realizada a los controles de acceso implementados en el sistema SIGO evidenciaron que se realiza el bloqueo de la información recogida en relación a las identificaciones a los 24 meses de su recogida. Además, a los seis meses desde su recogida se restringe el acceso a la misma a titulares de permisos específicos.

En cuanto al desvío de finalidad que podría suponer la utilización de dichos datos para evaluar la productividad de los Guardias Civiles destinados en servicios de identificación de personas, los resultados de la inspección evidenciaron que no es posible extraer del propio sistema la información necesaria para realizar dicho tratamiento.

No obstante, en atención a la relevancia del tratamiento de los datos de carácter personal por parte de las Fuerzas y Cuerpos de Seguridad del Estado, y con el fin de reforzar las garantías previstas en la normativa de protección de datos, la Agencia procedió a formular a la Dirección General de la Guardia Civil las siguientes recomendaciones:

- Homogeneizar los criterios objetivos sobre la incorporación de datos de personas sin antecedentes penales ni policiales.

- Establecer criterios temporales y materiales para la supresión de los datos en dicho fichero de conformidad con lo previsto en los artículos 4.5 y 22.4 de la LOPD.

- Armonizar los procedimientos para acreditar el cumplimiento del deber de información previsto en el artículo 5 de la LOPD en los supuestos no excluidos por el artículo 24.1 de la misma.

En cuanto a las solicitudes de **tutela de derechos**, estas han disminuido un 8,94% con respecto a 2012. Ocupan un año más el primer lugar las solicitudes de derecho de cancelación (1.300) seguidas de las referentes al derecho de acceso (594).

Además, se consolida al alza la relevancia que los ciudadanos otorgan al ejercicio de su derecho de borrado de datos, cuya solicitud crece respecto a 2012 (1.300 frente a 1.202) a pesar del descenso global en el número de tutelas presentadas (1.997 frente a 2.193 en 2012).

Los ciudadanos en España han sido pioneros en el ejercicio del denominado derecho al olvido (derecho de cancelación y oposición) para evitar la difusión universal y permanente de sus datos en Internet.

Desde el año 2007, en que se plantearon las primeras reclamaciones, su número ha mantenido un crecimiento constante aproximándose en 2012 a las 200 (199). En 2013 se aprecia una consolidación del número de reclamaciones recibidas (184), si bien con un incremento de las resueltas (181 en 2012 y 226 en 2013).

El mayor número de reclamaciones resueltas (157) se han dirigido frente a los prestadores de servicios de búsqueda en internet, lo que pone de manifiesto que la mayor inquietud de los ciudadanos se refiere a las facilidades de acceso a su información personal que proporcionan estos servicios, posibilitando su difusión universal y permanente. El ejercicio de los citados derechos no supone su reconocimiento automático, sino que es necesario valorar las circunstancias concurrentes en cada caso.

En 2013 el promedio de resoluciones estimatorias de las reclamaciones de los ciudadanos ascendió al 26,10%, porcentaje que es superior en relación con los Boletines y diarios oficiales (45,65%) e inferior respecto de los buscadores en internet (22,29%) y los medios de comunicación (13,04%).

Desde el momento en que los ciudadanos iniciaron reclamaciones sobre el ejercicio de estos derechos, se han planteado ante la Audiencia Nacional 226 recursos por la empresa Google contra las resoluciones estimatorias dictadas por la Agencia.

En relación con ellas la Audiencia Nacional planteó varias cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea (TJUE), que han sido resueltas finalizado el periodo que comprende esta Memoria por Sentencia de 13 de mayo de 2014.

El TJUE respalda las tesis de la AEPD en relación con el derecho al olvido en internet respecto del servicio de buscador de Google.

A continuación se mencionan las reclamaciones de tutela de derechos más destacadas resueltas por la Agencia en 2013:

- **Acceso a grabación del consentimiento en casos de portabilidad (TD/01107/2013)**

La entidad no contesta a la solicitud de acceso. En las alegaciones manifiesta que será enviada en los

próximos días al reclamante la carta de contestación, adjuntando un CD con la «grabación de verificación por terceros de la solicitud de portabilidad». Sin embargo, el reclamante en sus alegaciones dice no haber recibido dicha carta. Se comprueba que la dirección que consta en la citada carta no se corresponde con la indicada por el reclamante, tanto en la solicitud como en la reclamación.

- **Ficheros de solvencia**

Se han planteado 465 reclamaciones relativas a ficheros de solvencia que, en su inmensa mayoría, han sido inadmitidas o desestimadas (444) pues las entidades han contestado conforme a la normativa de protección de datos. Debe significarse que es el acreedor –y no el fichero de solvencia– el encargado de confirmar o no la deuda, no resultando competente la Agencia para analizar la misma. No obstante, la Agencia también tutela los casos en que el responsable del fichero de solvencia no da acceso a los datos del reclamante (TD/01599/2012).

- **Cancelación de antecedentes policiales (TD/01326/2013)**

La solicitud de un ciudadano para la cancelación de antecedentes policiales se deniega genéricamente invocando la aplicación de los artículos 22 y 23 de la LOPD. La tutela solicitada ante la Agencia estima la reclamación requiriendo que se especifiquen las razones de la denegación atendiendo a las circunstancias del caso planteado.

- **Cancelación frente a Facebook (TD/01021/2013)**

Un reclamante solicita la cancelación de sus datos personales frente a esta red social. Facebook Spain alegó, en síntesis, lo siguiente:

- La entidad frente a quien se tramita la tutela de derechos, Facebook Spain, no tiene control sobre los servicios de Facebook, por lo que se dio traslado a Facebook Ireland Limited, el proveedor del servicio de los usuarios de Facebook España y de la Unión Europea.

- Facebook Ireland una vez examinada la reclamación, procedió a eliminar el contenido.

Se estimó por motivos formales el procedimiento de tutela de derechos al haber atendido el derecho, aunque extemporáneamente.

- **Buscadores: captación de una noticia obsoleta (TD/01065/2013)**

Se insta a Google a que adopte las medidas necesarias para retirar de su índice el enlace a una publicación en un periódico en 1983 del proceso por un posible delito de imprudencia con resultado de muerte.

- **Publicación en el BOE de una notificación de sanciones (TD/01270/2013)**

La reclamante solicitó ante la Agencia Estatal del Boletín Oficial del Estado (BOE) la oposición al tratamiento de sus datos personales que aparecían en la página web sobre dos publicaciones en el BOE en las que se hace referencia a dos anuncios por notificación infructuosa de la Dirección General de la Marina Mercante, acordando el inicio de un expediente administrativo sancionador de 2007 y 2008.

Se consideró que dado el tiempo transcurrido desde la publicación en el Boletín y no concurriendo interés público en la puesta indiscriminada a disposición de terceros de la información personal afectada, asiste al reclamante un motivo legítimo

y fundado en el mantenimiento de su privacidad y en el consecuente deseo de limitar el acceso a la información relativa a su persona.

La AEPD procedió estimar la reclamación de tutela de derechos instando al BOE a la adopción de medidas para evitar la indexación por buscadores.

- **Imágenes de vídeo (TD/01424/2012)**

La reclamante es una bailarina que indica que un vídeo alojado en la plataforma YouTube, grabado y publicado sin su consentimiento, le está provocando graves perjuicios personales al incluir un beso a una compañera.

La resolución estima la reclamación en orden a la cancelación de los datos publicados en el vídeo.

En sentido contrario, diversas resoluciones dictadas en 2013 han perfilado el alcance de los derechos ARCO especificando los supuestos en los que no procede la estimación de lo solicitado.

- **Procedimientos especiales de cancelación (TD/01474/2013)**

Se solicita la cancelación por el procedimiento previsto en la LOPD, en un supuesto regulado por una ley que establece un procedimiento especial para la rectificación o cancelación de los datos. Conforme al art. 28.5 del RLOPD deben aplicarse los procedimientos especiales. Entre ellos se encuentran los procedimientos de rectificación y cancelación en materia de Seguridad Social, puntos de tráfico, expedientes académicos o seguros.

- **Cancelación de certificado de firma electrónica (TD/01638/2013)**

Un trabajador de un organismo público solicitó la cancelación de la *«Solicitud de emisión de certificado de firma electrónica de empleado público de la que soy firmante y custodio y cuyo registrador es D. (…)»*.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en su artículo 19.2, «Firma electrónica del personal al servicio de las Administraciones Públicas», determina que cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica.

El certificado de firma electrónica de empleado público sobre el que solicita la cancelación es una herramienta puesta a su disposición por el organismo para el que presta servicios para su identificación como trabajador, siendo, por ello, una condición obligatoria en su relación laboral.

- **Solicitud de direcciones IP que se conectan (TD/02152/2012)**

El reclamante remitió escrito a Google requiriendo *«Información de la relación de las direcciones IP que se han conectado de forma masiva para hacer subir en el buscador la información fraudulenta, para conocer si además de la publicación irregular también han existido ataques masivos al buscador para subirla en el ranking para hacer que la información calumniosa se difunda de forma intensiva para hacerme el máximo daño posible. Les solicito el estadístico de las direcciones IP y las fechas en que han accedido a Google consultando mi nombre, estadístico que dirá si alguien pudo estar detrás de actividades fraudulentas (…)»*

No se tuteló el derecho al considerar que la pretensión no era la obtención de sus datos personales, tal como establece la normativa de protección de datos, sino de terceras personas, quedando, por tanto, fuera del objeto del procedimiento de tutela de derechos.

■ **Oposición a la publicación en el BOE del nombramiento de funcionarios** (TD/1802/2012)

En el caso suscitado –funcionarios de Correos– no cabía deducir, ni se ha invocado ni ha quedado acreditada la existencia de motivo legítimo y fundado que, refiriéndose a una situación personal, justifique el derecho de oposición solicitado. No se deduce que existan implicaciones de seguridad por el sector al que pertenece en el hecho de que su nombramiento siga siendo accesible a través de buscadores, a diferencia de otras tutelas tramitadas referentes a funcionarios de la Fuerzas y Cuerpos de Seguridad o vigilantes de seguridad (TD/01269/2013) que, por las razones aducidas, han derivado en estimación de la tutela. (TD/01239/2013).

■ **Relevancia pública (TD/02027/2012, TD/02028/2012 y TD/02029/2012)**

Inadmisión de tres solicitudes de tutela del mismo reclamante por su relevancia pública. El afectado estaba implicado en casos conocidos de corrupción.

■ **Acceso al historial clínico**

Por otra parte, han revestido especial relevancia las solicitudes de tutela por acceso a historial clínico incompleto. Ante las reclamaciones de tutelas por acceso a historial clínico otorgado de forma incompleta se opera según los siguientes criterios:

Se desestima en los siguientes casos:

- Si no está probado el acceso incompleto, ni se especifican cuáles son los documentos que no se han entregado a los reclamantes ni se sustenta tal pretendida ausencia en medio probatorio alguno.
- En el caso de que afirme que faltan determinados documentos (hoja de evolución de medicina y enfermería…) y la clínica lo niega.
- Si lo que solicita son «valoraciones o apreciaciones de índole médico» al no considerarse como datos de base del afectado (TD/01492/2013).
- Si rebasa los límites que según el artículo 18.3 de la Ley de Autonomía del Paciente es necesario tener en cuenta:
  - – El derecho de terceras personas a la confidencialidad de los datos que constan en el documento y que se hubieran recogido en interés terapéutico del enfermo.
  - – El derecho de los profesionales que han participado en la elaboración del historial de retirar sus anotaciones subjetivas.

Se estima si está acreditado o probado el acceso incompleto cuando:

- Le facilitan un resumen o un informe.
- Es ilegible (letra manuscrita).
- Se deduce del expediente sin esfuerzos desproporcionados (TD/101449/2013) que la clínica rechaza el acceso porque señala que «*no es posible facilitarle el acceso al informe pericial ya que al mismo se aplican conocimientos técnicos para su elaboración siendo propiedad de la entidad que lo realiza*».
- Frente a la invocación de que el historial clínico está incompleto, el responsable no ha manifestado alegación alguna.

Finalmente, en ejecución de una sentencia de la Audiencia Nacional se ha dictado en 2013 una resolución derivada de la TD/1781/2009 relativa a la

naturaleza de los **motores de búsqueda internos de los periódicos digitales.**

En cumplimiento de la sentencia se analizó la naturaleza de los motores de búsqueda que se incluyen en la página web de los diarios digitales y se subrayaron dos circunstancias: su carácter de prestación interna habilitada por el propio medio y el hecho de que se utiliza una vez que el usuario ha accedido a su página web para canalizar una información ya incluida en los propios medios de comunicación.

Los buscadores internos son instrumentos inherentes a los diarios que facilitan al usuario el acceso a la información del periódico, no existiendo un tratamiento externo como ocurre con los buscadores existentes en internet. Son los propios medios los que deciden sobre su existencia o no y acerca de los criterios de implementación, modulando el acceso al conocimiento de los contenidos informativos del periódico.

Desempeñan, además, una función que únicamente se despliega tras haber procedido el usuario voluntariamente a acceder al medio de comunicación: obtener la información disponible en la web del medio realizando funciones semejantes a las de un índice en una dirección impresa.

En consecuencia, dichos motores se utilizan una vez que se ha accedido al diario digital (son buscadores internos), son implementados por el propio medio y sirven para conocer, con mayor rapidez, las noticias que ya están recogidas en los mismos una vez que se ha comenzado a navegar en sus páginas. Una vez que se ha accedido a su web, sólo tratan los datos de personas sobre las que hay noticias, esto es, sólo sirven para obtener información sobre datos ya publicados por el medio de comunicación afectado.

Estas circunstancias les inviste de la misma legitimidad que ampara a la información que se obtiene de su utilización, debiendo considerarse que quedan acogidos también por las previsiones del artículo 20.d) de la Constitución.

En cuanto a la **exención del deber de información**, debe señalarse que, junto a los procedimientos citados anteriormente, en 2013 se han resuelto cuatro solicitudes de este tipo por exigir esfuerzos desproporcionados al responsable del tratamiento (art. 5.5 LOPD).

Entre ellos destaca la relativa al procedimiento A5/00004/2013, derivada de una resolución del Tribunal de Defensa de la Competencia (TDC) que, en ejecución de una incidencia de cumplimiento de un procedimiento sancionador a una empresa energética por prácticas restrictivas de la libre competencia, determina que debía proporcionar los datos de sus clientes a las entidades instaladoras de gas homologadas que se lo soliciten de cara a efectuar la revisión periódica de las instalaciones de gas de los clientes que se hace cada 5 años. La empresa llevaba transfiriendo los citados datos a sus franquiciadas y el TDC impuso para que se compita en igualdad de condiciones que se proporcionasen también a los instaladores autorizados los datos de esos clientes, ya que estos pueden efectuar esta revisión con la empresa con la que deseen, no informándose a los clientes que podrían contratar la revisión libremente.

La Agencia consideró que la cesión estaría legitimada por intereses legítimos del cedente o cesionario siempre que se informe a los afectados.

La empresa pidió que se relevara la exigencia de informar personalmente a más de 7 millones de clientes de este tipo de producto por el alto coste y por no tener otro mecanismo alternativo de infor-

mación, pues los domicilios del suministro suelen ser segundas residencias o personas mayores en entornos rurales.

De las 4 solicitudes presentadas, esta fue la única en la que se concedió la exención del deber de informar previsto en la LOPD.

En lo referente al ámbito de competencias de la AEPD, en 2013 han tenido lugar tres importantes novedades.

- **Asunción de las competencias de la Agencia de la Comunidad de Madrid**

El artículo 61 de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas, de la Comunidad de Madrid, suprimió —con fecha de efectos de 1 de enero de 2013—, la Agencia de Protección de Datos de la Comunidad de Madrid.

Las competencias de la extinta Agencia madrileña se han reintegrado al ámbito estatal, correspondiendo su ejercicio a la Agencia Española de Protección de Datos.

- **Remisión al Consejo General del Poder Judicial de denuncias frente a ficheros de órganos jurisdiccionales**

En cumplimiento de lo dispuesto por el Tribunal Supremo en su Sentencia de 2 de diciembre de 2011, en la que resuelve que el ejercicio de las competencias relacionadas con la aplicación de la LOPD a los ficheros bajo responsabilidad de los órganos judiciales corresponde al Consejo General del Poder Judicial, se ha procedido a remitir a esa Institución 33 expedientes de denuncias y 5 expedientes de tutela que fueron presentadas ante la Agencia Española de Protección de Datos.

En este ámbito, en la reforma de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, llevada a cabo por la Ley Orgánica 4/2013, de 28 de junio, ha modificado las atribuciones del Consejo General del Poder Judicial, incluyendo la de «colaborar con la Autoridad de Control en materia de protección de datos en el ámbito de la Administración de Justicia. Asimismo, asumirá las competencias propias de aquélla, únicamente respecto a la actuación de Jueces y Magistrados con ocasión del uso de ficheros judiciales» (art. 560.1.19).

- **Notificación de quiebras de seguridad**

En el mes de agosto de 2013 entró en vigor el Reglamento (UE) N.º 611/2013 de la Comisión, de 24 de junio, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. En este documento se desarrolla una obligación que ya se había incorporado el año anterior al ordenamiento jurídico español a través de la modificación del artículo 34 de la LGT, donde se designaba a la Agencia Española de Protección de Datos como la Autoridad a la que los operadores de servicios de comunicaciones electrónicas deben notificar las eventuales quiebras de seguridad de datos personales que puedan producirse en sus sistemas.

C - LA SEGURIDAD JURÍDICA COMO OBJETIVO PRIMORDIAL

La AEPD ha continuado trabajando en el objetivo de lograr mayor seguridad jurídica a través de los informes preceptivos sobre disposiciones de carácter general, dirigidos a mejorar la sistemática del ordenamiento jurídico integrando una norma de carácter transversal con las regulaciones sectoriales.

De este modo fueron informadas 139 disposiciones de carácter general, lo que supone un máximo en el número de disposiciones sujetas a informe, con un incremento del 45% respecto del ejercicio anterior. Dicho incremento se debe en parte a la emisión de 19 informes a disposiciones provenientes de la Comunidad de Madrid, como consecuencia de la supresión de su Agencia autonómica de protección de datos. No obstante, descontado el efecto de dichas disposiciones, el incremento sigue siendo de un 25% respecto a 2012.

De entre las disposiciones informadas por la Agencia cabe hacer referencia a las siguientes:

- Anteproyecto de Ley Orgánica de Seguridad Ciudadana.
- Anteproyecto de Ley de Ley General de Telecomunicaciones.
- Anteproyecto de Ley de Garantía de la Unidad de Mercado.
- Anteproyecto de Ley de Asistencia Jurídica Gratuita.
- Anteproyecto de Ley de Reforma de la Ley de Propiedad Intelectual y la Ley de Enjuiciamiento Civil.
- Anteproyecto de Ley de Seguridad Privada.
- Anteproyecto de Ley de Servicios y Colegios Profesionales.
- Proposición de Ley de reforma de la Ley General Tributaria en relación con la publicidad de los datos referidos a los procedimientos extraordinarios de regularización fiscal.
- Propuesta de modificación de la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, en lo relativo a la modificación del régimen de la central de información de riesgos del Banco de España (CIRBE), elaborado a instancia de dicha Institución.
- Proyecto de Real Decreto por el que se regulan los ensayos clínicos con medicamentos, Comités de ética y Registros de estudios clínicos.
- Proyecto de Real Decreto de garantía de la asistencia sanitaria transfronteriza.
- Proyecto de Real Decreto de reforma del Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia y se crea el fondo documental de requisitorias.
- Proyecto de Real Decreto Legislativo por el que se aprueba el Texto Refundido de la Ley General de Derechos de las personas con discapacidad y su inclusión social.
- Proyecto de Real Decreto de reforma del Reglamento Hipotecario en materia de venta forzosa extrajudicial.
- Proyecto de Real Decreto por el que se regula el Registro Estatal de Profesionales Sanitarios.
- Proyecto de Real Decreto por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.
- Proyecto de Orden por la que se regula el Sistema para la autonomía y atención a la dependencia.
- Proyecto de Orden por la que se modifican los anexos I, II, III y IV del Real Decreto 1675/2012, de 14 de diciembre, por el que se regulan las recetas oficiales y los requisitos especiales de

<Índice>

prescripción y dispensación de estupefacientes para uso humano y veterinario.

- Proyecto de Orden de creación del registro Electrónico Común de la Administración General del Estado.

- Proyecto de Orden de creación del Tablón Edictal de la Inspección de Trabajo y de la Seguridad Social.

- Proyecto de Orden por la que se define la cartera común suplementaria de transporte sanitario no urgente del Sistema Nacional de Salud.

- Proyecto de Orden de modificación de la Orden de 25 de febrero de 2000, reguladora del Índice Nacional de Defunciones.

- Proyecto de Circular del Banco de España sobre la Central de Información de Riesgos (CIR) y por la que se propone la modificación de la Circular 4/2004, de 22 de noviembre, sobre Normas de información financiera pública y reservada y modelos de estados financieros.

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.

Durante el año 2013 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 274 sentencias, de las cuales:

- 179 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia, que quedaron plenamente confirmadas (65%).

- 33 estimaron parcialmente los recursos (12%).

- 53 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (20%).

- 9 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (3%).

Es preciso en este punto clarificar que de las 33 sentencias parcialmente estimatorias dictadas en el año 2013, 9 lo han sido como consecuencia de la aplicación retroactiva del régimen sancionador de la LOPD establecido por la disposición adicional quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible. Su entrada en vigor, como se ha indicado en memorias de ejercicios anteriores, ha conducido a que la Audiencia Nacional haya apreciado que concurrían los requisitos legalmente exigidos para que procediera esa aplicación retroactiva, lo que ha supuesto en 8 ocasiones la rebaja de la sanción de 60.000 a 40.000 euros, como consecuencia de la rebaja de la cuantía inferior de las sanciones correspondientes a la comisión de infracciones graves, y en una la aplicación retroactiva de los criterios de atenuación contenidos en el nuevo artículo 45.5 de la LOPD.

De este modo, cabe concluir que la confirmación de los criterios de la Agencia en cuanto al fondo del asunto ha sido de un 72%, incrementándose así en un punto porcentual sobre la del año 2012 y siendo por tanto similar a la de los años 2010 y 2011.

En relación con los sectores de actividad a los que afectan las sentencias dictadas, continúa creciendo el peso del sector de las telecomunicaciones con un incremento del 43% respecto a 2012. Las 119 sentencias relativas a este sector suponen, además, el 43% del total de las dictadas en 2013.

Es también muy notable el número de recursos interpuestos por particulares, bien contra resoluciones desestimatorias de tutelas, bien contra resoluciones de archivo de actuaciones, que se mantienen en la misma cifra que en 2012.

Debe asimismo ponerse de manifiesto el enorme incremento de las sentencias dictadas en recursos interpuestos por entidades pertenecientes al sector eléctrico y gasista (de un 320% en 2013, pasando de un 3% a un 8% del total), el también notable incremento de un 150% de las recaídas en recursos interpuestos por partidos políticos y sindicatos, y del 125% en las relacionadas con entidades del sector financiero.

Igualmente se incrementa el número de recursos interpuestos por entidades gestoras de ficheros de solvencia patrimonial y crédito, que se ha incrementado en un 70% respecto del año anterior, que debe añadirse al incremento del 67% producido en 2012.

Por su parte, disminuye el número de recursos relativos a prestadores de servicios de la sociedad de la información, volviendo a ser significativo el número de recursos relacionado con las entidades dedicadas a la publicidad y prospección comercial (aunque sólo alcanza un 2% del total).

En cuanto a las materias, se pueden destacar las referidas a la inclusión de datos inexactos en ficheros de solvencia patrimonial y crédito o a la contratación de servicios.

También es preciso indicar que en un buen número de sentencias estimatorias la decisión final del recurso se ha fundado en la ampliación, mediante la prueba practicada en el ámbito del recurso, de la llevada a cabo 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.

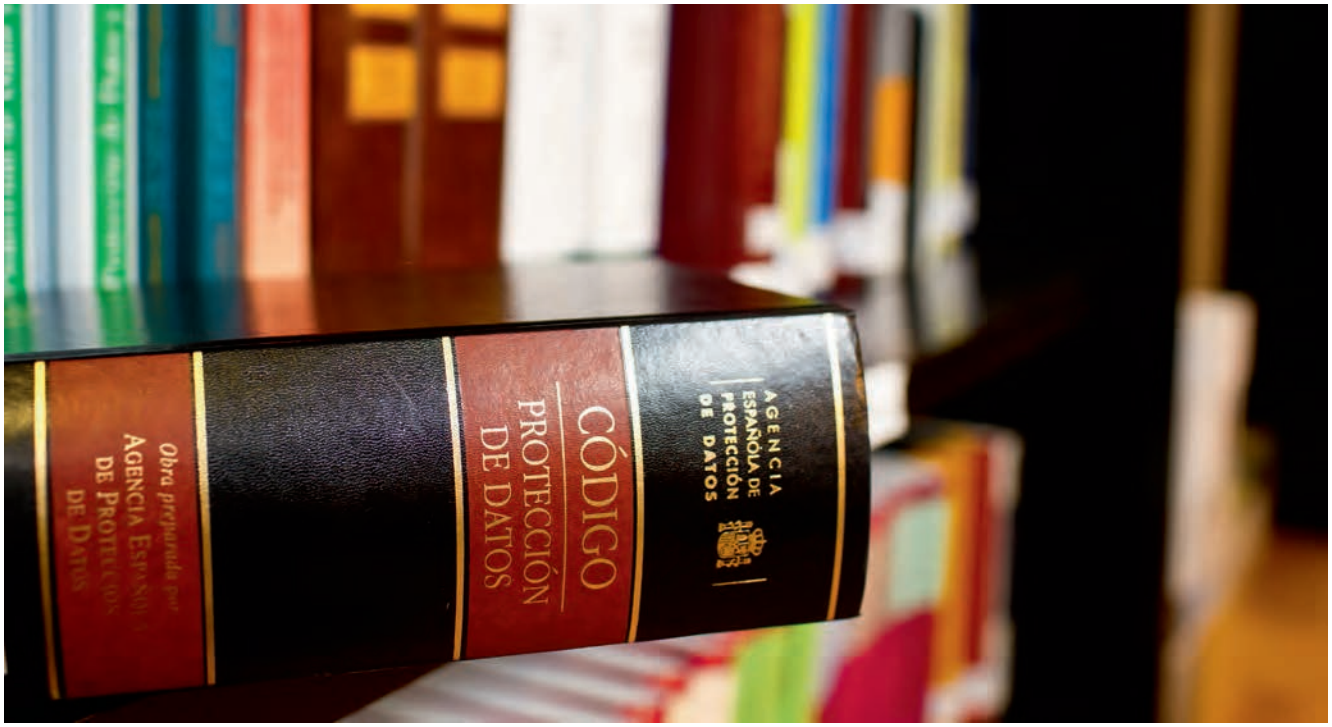
De las materias analizadas por la Audiencia Nacional destacan las siguientes cuestiones:

- En relación con los conceptos generales en materia de protección de datos, la Audiencia Nacional ha entendido que la existencia de un fichero está implícita en el ejercicio de la actividad de asesoría jurídica (SAN 19/7/2013). Asimismo, la SAN 9/7/2013 ha considerado el número de cuenta corriente un dato personal, incluso no asociándose a su titular.

- En cuanto al ámbito de aplicación de la LOPD, la AN ha puesto de manifiesto en la SAN 4/10/2013 que el hecho de que las personas jurídicas no sean titulares del derecho a la protección de datos no contraviene ni la CE ni el Convenio 108 del Consejo de Europa. Igualmente las SSAN de 25/10/2013 y 11/12/2013 han analizado el alcance de la excepción contemplada en el artículo 2.3 del RLOPD, considerando en ambos casos que el tratamiento de los datos de los afectados está sometido a la LOPD.

- Sobre la existencia de legitimación para el tratamiento fundada en la existencia de un interés legítimo prevalente del responsable, la AN ha ponderado la prevalencia del derecho a la libertad de información en sus sentencias de 10/5/2013 y 3/12/2013 (entendiendo por el contrario que dicha libertad no prevalece sobre la protección de datos en la sentencia de 29/11/2013). También ha valorado que no puede entenderse prevalente el derecho a la libertad sindical en un supues-

<Índice>



to de publicación «en abierto» y con posible acceso a través de motores de búsqueda del censo electoral sindical de una Administración Pública (SAN 28/10/2013) y ha mantenido el criterio que venía sustentando en relación con la prevalencia del derecho a la tutela judicial efectiva en el tratamiento por los abogados de los datos de la parte contraria en SAN 15/10/2013.

■ Son relevantes las sentencias en que la AN ha desestimado los recursos contra resoluciones de la AEPD en las que se declaraba no haber lugar a las solicitudes de los afectados de que se procediera a la anonimización de las SSTC publicadas en el BOE que contenían sus datos personales (SSAN 19/7/2013 y 11/11/2013) o solicitaban asimismo la aplicación sobre las mismas de protocolos de exclusión de motores de búsqueda (SSAN 26/9/2013 y 30/10/2013). En todos los casos, la AN ha entendido que la ponderación de los derechos e intereses en juego corresponde realizarla al TC como intérprete supremo de la CE, que había desestimado estas solicitudes de ejercicio de derechos.

■ Son igualmente numerosas las SSAN referidas a supuestos concretos en los que se ha valorado si existe otra causa legitimadora del tratamiento, siendo su conclusión negativa en casos como la publicación de fotografías de asistentes a un congreso en la página web de la empresa a la que se había encargado su organización (SAN 27/9/2013), la inclusión de los datos de un abonado en la guía cuando había manifestado su deseo de no inclusión (SAN 20/9/2013), la apertura por una entidad financiera de una cuenta para domiciliación de

nóminas como consecuencia de un acuerdo con el empleador sin contar con el consentimiento del trabajador (SAN 21/3/2013) o la contratación por un mediador de una póliza de seguro para su cliente sin haber requerido su consentimiento (SAN 14/6/2013).

- En relación con el posible tratamiento de datos contenidos en resoluciones judiciales, la SAN 29/11/2013 reitera el criterio de que la publicidad de dicha resoluciones lo es sólo para conocimiento de las partes, no legitimando su tratamiento indiscriminado.

- Vuelven a ser muy abundantes los supuestos relacionados con la contratación de servicios. En este punto es preciso señalar que la AN ha reiterado que la imputabilidad puede recaer tanto en la empresa distribuidora, como encargada del tratamiento, que debe actuar con la debida diligencia (SAN 17/7/2013), como en la empresa prestadora de los servicios contratados, en su condición de responsable del tratamiento (SAN 30/12/2013), aplicando este criterio igualmente a las entidades de seguros respecto de la conducta de sus agentes mediadores (SAN 20/11/2013). Asimismo, ha apreciado que en estos supuestos no cabe acumulación, de modo que cada supuesto de contratación irregular implica la comisión de una infracción distinta y que no cabe exigir al denunciante la prueba de la no celebración, al tratarse de una prueba diabólica (SAN 9/10/2013).

- En cuanto a la apreciación de la existencia de indicios de contratación, se ha considerado que concurren en casos tales como el abono reiterado de los servicios contratados (SAN 10/4/2013), la aportación de grabaciones referidas a la verificación del contrato (SAN 28/6/2013 y 8/11/2013), la apreciación de un error excusable no pudiendo exigirse mayor diligencia, al haberse producido una contratación fraudulenta por un distribuidor condenado penalmente por ello (SAN 3/10/2013) o el tratamiento de datos que aparentemente sólo podía aportar el afectado (SAN 28/10/2013).

- Por el contrario, se ha negado la existencia de prueba en caso de contratación de anteriores titulares del servicio (SSAN 20/9/2013 y 26/12/2013) o el uso de datos de un cliente para la contratación de nuevos servicios sin que conste su solicitud (SAN 11/10/2013, en que figuraba otro nombre pero el DNI de un cliente). Asimismo, la SAN 30/12/2013 se refiere a un supuesto de contratación presencial en que la distribuidora no puede aportar el DNI cuando las normas internas de funcionamiento así lo exigen. También se ha apreciado que no hay contrato en el caso de contratación de seis líneas telefónicas a nombre de un mismo abonado apareciendo firmas totalmente distintas en todos ellos (SAN 13/9/2013), el supuesto de contratación electrónica reiteradamente denunciada por el afectado, conforme a grabaciones aportadas (SAN 13/9/2013) o declarándose su inexistencia por una OMIC (SAN 10/12/2013), o contratos que no están firmados (SAN 11/11/2013).

- Por otra parte, las SSAN 11/10/2013, 29/10/2013 y 4/11/2013 han puesto de manifiesto que la gestión de cobros puede exceder de un mero encargo del tratamiento si se establecen especialidades contractuales que otorgan a la entidad un mayor margen de actuación y gestión de la información a la empresa de recobros.

<Índice>

■ En cuanto al ejercicio de derechos, debe partirse de que la AN ha puesto reiteradamente de manifiesto que corresponde al interesado la prueba de su ejercicio ante el responsable del fichero (SSAN 20/11/2013 y 3/12/2013). A su vez, la AN ha señalado que las normas reguladoras del derecho de cancelación no pueden considerarse el cauce adecuado para instar la cancelación de los datos relativos a las sanciones impuestas por un determinado regulador (SAN 1/7/2013). En cuanto al ejercicio del derecho de oposición respecto de informaciones publicadas en medios de comunicación, la AN, en sentencia de 9/12/2013, considera que, sin perjuicio de la libertad de información, la AEPD sí puede valorar la procedencia de que el medio aplique protocolos de exclusión de la información de motores de búsqueda.

■ En el ámbito de las historias clínicas, la SAN de 6/11/2013 ha indicado que las pruebas diagnósticas, como radiografías, TACs, etc. deben encontrarse incorporadas a la historia y el interesado, o en caso de haber fallecido éste las personas habilitadas para ello conforme a la Ley de Autonomía del Paciente, deben poder acceder a esos datos.

■ En el ámbito de la seguridad, la AN ha apreciado su vulneración en supuestos en que los datos eran accesibles al otorgar el sistema un usuario y contraseña por defecto (SAN 2/7/2013) o en caso en que la migración de un sistema hizo visibles datos de terceros (SAN 29/11/2013). En todo caso, considera preciso acreditar la existencia efectiva de un fallo en la seguridad para que proceda sancionar la infracción (SAN 28/6/2013).

■ La AN ha entendido vulnerado el deber de secreto en caso de revelación de los movimientos de la cuenta de un fallecido y su sobrino heredero universal a otro familiar que no era heredero (SAN 29/5/2013) o en la realización por el acreedor de llamadas a un familiar del deudor poniendo de manifiesto la deuda y su cuantía (SAN 22/4/2013).

■ En cuanto a los ficheros de solvencia son diversas las sentencias referidas a la falta de certeza de la deuda por la existencia de un litigio civil sobre la misma (SAN 13/12/2013), un acuerdo transaccional por la que se redimía parcialmente al deudor (SAN 12/7/2013), diligencias previas no archivadas seguidas contra el acreedor por un presunto delito de estafa (SAN 22/11/2013), o reclamaciones seguidas ante las Juntas Arbitrales de Consumo, incluso aportándose un laudo estimatorio (SSAN 15/10/2013 y 6/11/2013) o la SETSI (SSAN 28/6/2013, 24/10/2013, 23/7/2013 y 9/12/2013).

■ También son muchas las sentencias relacionadas con el cumplimiento del requisito previo del requerimiento de pago, no considerándose válido el efectuado por SMS, dado que no puede probarse ni su recepción ni su lectura por el deudor (SAN 14/11/2013). Además, el requerimiento debe expresar que en caso de no ser atendido se procederá a la inclusión (SAN 25/10/2013), no siendo válida la inclusión de datos antes de cumplirse el plazo establecido en el requerimiento (SAN 15/11/2013).

■ Han sido numerosas las sentencias relacionadas con el tratamiento de datos con fines de videovigilancia, partiendo de lo señalado en la SAN 20/9/2013, que considera plenamente compatible lo previsto en la Instrucción 1/2006

con el artículo 7 f) de la Directiva 95/46/CE, al considerar que la ponderación prevista en ese precepto se lleva a cabo mediante la aplicación de la regla de proporcionalidad, según las circunstancias de cada caso concreto (en los mismos términos SAN 20/11/2013). Por otra parte, la Audiencia entiende que no cabe amparar la grabación en la protección de la salud o la higiene, sino sólo en la seguridad (SAN 20/11/2013).

- En relación con la proporcionalidad en estos tratamientos, la AN la ha apreciado en el supuesto de una compañía logística de distribución de tabacos, en que las cámaras captan la vía pública para vigilar la entrada y evitar el robo (SAN 20/11/2013), en la grabación de las zonas aledañas a una instalación que no está en núcleo urbano con el fin de controlar el vandalismo (SAN 26/12/2013) o en las meras reproducciones en tiempo real efectuadas por un monitor situado en la entrada de un comercio que se limita a reproducir imágenes que son igualmente visibles por el ojo humano sin necesidad del monitor (SAN 25/10/2013). Sin embargo, ha considerado desproporcionada la captación de la vía pública aledaña a un edificio en núcleo urbano, que incluía la calzada, pudiendo captar a todos los viandantes de la acera (SAN 20/9/2013) o la grabación de imágenes en duchas, taquillas y piscinas de un centro de ocio (SAN 20/11/2013).

- En el marco de las actividades de publicidad y prospección comercial cabe hacer referencia a dos sentencias: la de 11/12/2013, según la cual la existencia de un contrato no legitima el envío de publicidad sobre productos similares si existe negativa a recibirla desde el momento de la celebración, y la de 17/5/2013, que considera válida la actuación de un encargado que se limita a depurar una base de datos de clientes con información de los mismos que aparece en fuentes accesibles al público.

- En relación con la aplicación de lo dispuesto en el artículo 21 de la Ley de Servicios de la Sociedad de la Información (LSSI), la AN ha puesto de manifiesto que las previsiones de esa norma son aplicables en todo caso, al margen de lo dispuesto en la LOPD, siendo irrelevante que la dirección a la que se envían las comunicaciones sea o no genérica y corresponda o no a una persona jurídica, e incluso que la misma sea accesible en la web de la entidad destinataria. Además, entiende que existen comunicaciones comerciales en los correos remitidos por un hotel sobre sus futuros eventos (SAN 9/12/2013), no siendo posible alegar la excepción de relación contractual (art. 21.2 LSSI) cuando el interesado se ha opuesto expresamente a recibir comunicaciones comerciales (SAN 18/10/2013).

- Por otra parte, la SAN de 19/7/2013 señala que la infracción consistente en la falta de notificación del fichero para su inscripción en el RGPD es una infracción persistente a efectos de prescripción, de forma que la prescripción sólo se interrumpe por la notificación.

- En cuanto a la aplicación de los criterios contenidos en el artículo 45.5 de la LOPD, la AN ha considerado que es preciso tener en cuenta circunstancias tales como la naturaleza del responsable (no procediendo su aplicación en el caso de una entidad financiera -13/12/2013-), los perjuicios al afectado (no procediendo en supuestos como la inclusión de los datos en ficheros de solvencia -SAN 13/12/2013-), la existencia de buena fe (SSAN 14/6/2013 y 21/3/2013), la rectificación inmediata de la conducta (SSAN 21/3/2013

y 9/10/2013), la existencia de una operación de absorción (29/11/2013), como en el caso de creación de sistemas institucionales de protección (SAN 26/6/2013), la concurrencia de circunstancias especiales como en los supuestos contemplados por las SSAN 23/7/2013 y 9/12/2013, en los que se sancionó la inclusión en ficheros de solvencia de deudas impugnadas ante la SETSI que finamente ésta consideró existentes, o el reconocimiento de la comisión de la infracción (SAN 29/11/2013).

- En cuanto al apercibimiento, la SAN 29/11/ 2013 considera que el mismo debe incluir medidas correctoras, recordando la SAN 12/6/2013 que en caso de que las mismas no sean comunicadas a la AEPD procederá la imposición de la correspondiente sanción. Por lo demás, la SAN 26/12/2013 recuerda que se trata de una medida excepcional, considerando que no procede atendiendo a la actividad a la que se dedica la infractora (mutua de accidentes) y a la infracción cometida (cesión de datos). En el mismo sentido se pronuncia la SAN 13/12/2013, referida a un supuesto de comunicación de datos a ficheros de solvencia por una entidad financiera.

- En cuanto a las cuestiones de carácter general o relacionadas con el procedimiento, la SAN 20/11/2013 considera que la falta de audiencia al afectado tras las alegaciones del responsable en el procedimiento de tutela es irregularidad no invalidante y la SAN 6/11/2013 señala que las resoluciones de estos procedimientos por motivos formales solo caben en caso de respuesta de responsable fuera de plazo. También deben señalarse las SSAN de 3/12/2013, que declaran que quien recurre una resolución de tutela no puede pretender la imposición de una sanción en el recurso contencioso-administrativo, y de 15/11/2013, que considera que no procede la apertura de un procedimiento sancionador cuando se denuncian unos hechos que podrían vulnerar la LOPD pero que aún no han tenido lugar, al no haberse cometido una infracción.

Por su parte, el Tribunal Supremo, dictó un total de 12 resoluciones (7 sentencias y 5 autos) referidas a recursos de casación o de casación para unificación de doctrina interpuestos frente a sentencias dictadas en procesos en los que era parte la Agencia. Es preciso poner de manifiesto que el número de recursos ha sufrido una drástica reducción como consecuencia de la reforma operada en la Ley 29/1998, reguladora de la Jurisdicción Contencioso-administrativa, por la Ley 37/2011, de 10 de octubre. De este modo, las sentencias dictadas en 2013 son ya sólo un tercio de las dictadas en 2012.

En relación con estos recursos, el Tribunal Supremo:

- Declaró en 7 sentencias no haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia, que quedaron así, a su vez, confirmadas.

- Acordó en 5 supuestos la inadmisión del recurso.

En consecuencia, los criterios de la Agencia que fueron objeto de conocimiento por el Tribunal Supremo fueron en todo caso confirmados por el Alto Tribunal.

DESAFÍOS PARA LA PRIVACIDAD: PRESENTE Y FUTURO

A - LA PRIVACIDAD COMO ELEMENTO CLAVE PARA CONFIAR EN LOS SERVICIOS DE INTERNET

La tecnología disponible permite recoger y almacenar cantidades ingentes de datos personales sin que, en buena parte de las ocasiones, el ciudadano sea consciente ni de la recogida en sí misma ni de las consecuencias de la combinación transversal de la información que facilita cuando utiliza servicios muy diferentes entre sí.

La concentración de información personal en manos de un número reducido de prestadores de servicios en internet ha sido y continúa siendo un elemento de riesgo para los usuarios de la Red y un motivo de preocupación para las Autoridades de Protección de Datos, ya que esa acumulación de enormes cantidades de información constituye, además, un estímulo adicional para que terceras entidades, públicas y privadas, pretendan acceder a ella y utilizarla para sus propios fines.

Las informaciones difundidas sobre las prácticas de las agencias de seguridad norteamericanas y los servicios secretos de algunos estados europeos evidencian la necesidad inaplazable de abordar en profundidad las garantías para el uso de esta información partiendo del escrupuloso respeto de los derechos fundamentales de las personas y, en particular, de la protección de los datos personales y la privacidad.

A esta misma conclusión puede llegarse respecto de uso de la información por parte de operadores privados.

La recuperación de la confianza de los clientes y usuarios de servicios en internet va a colocar la protección de sus datos en una posición central en la configuración de los modelos de negocio de la economía digital durante los próximos años. En esta perspectiva, la protección de los datos de los usuarios correctamente aplicada de modo que se adapte de forma flexible a los servicios que se desarrollen, no sólo no es un obstáculo para la innovación y el desarrollo, sino que es una condición necesaria para generar confianza en los bienes y servicios que se ofrezcan. Es, por ello, necesario afirmar lo equivocado que resulta sostener que la protección de los datos personales y la privacidad son un elemento inhibidor de la economía digital y del comercio en internet. Por el contrario, debe reafirmarse el principio de que sin protección de los usuarios no se generaría confianza y que sin confianza de los usuarios y clientes no es posible desarrollar un modelo de negocio sólido.

En la consecución de este objetivo, la articulación de una relación constante y fluida entre la industria y las Autoridades de Protección de Datos personales debe asumirse como una premisa insoslayable.

Por otra parte, los retos planteados, por su naturaleza global, hacen imprescindible un avance cualitativo en la cooperación de las Autoridades de Protección de Datos de la Unión Europea que haga posible una respuesta común para garantizar los altos niveles de protección de la privacidad de los ciudadanos europeos. Cooperación que, junto a la adopción de criterios comunes para la protección de los datos personales, debe aportar avances significativos en la adopción de decisiones que permitan hacer efectiva dicha protección.

B - EL RESPETO A LA PRIVACIDAD COMO LÍMITE DE LAS AUTORIDADES PÚBLICAS

Uno de los principales retos para la recogida, acceso y uso de los datos personales por parte de

<Índice>

las autoridades públicas proviene de la tradicional tensión entre libertad y seguridad. Este reto ha alcanzado una intensidad sin precedentes como consecuencia de las posibilidades de acumulación y análisis masivo de información con las tecnologías disponibles, cuya rápida evolución hace previsible que se incrementen exponencialmente en un futuro próximo.

En junio de 2013, a través de las revelaciones del diario británico *The Guardian* y de otros medios europeos, se tuvo conocimiento de la existencia de diversos programas de vigilancia electrónica desarrollados por la Agencia Nacional de Seguridad de los EEUU, así como por el FBI, la CIA y varios servicios de inteligencia europeos. En el caso de las agencias norteamericanas, estos programas, principalmente el denominado PRISM, estarían dirigidos prioritariamente a la vigilancia de las comunicaciones de ciudadanos no norteamericanos, entre los que, según las informaciones conocidas, se encuentran datos de ciudadanos europeos. En el caso de PRISM, podría haberse accedido a datos recogidos en todo el mundo por grandes compañías de internet que se almacenan en servidores radicados en territorio estadounidense junto con accesos a través de otros mecanismos.

A la vista de la gravedad de las informaciones difundidas, el Grupo de Autoridades Europeas de Protección de Datos (GT29) reaccionó inmediatamente mediante el envío de una primera carta de su Presidente a la vicepresidenta de la Comisión Europea, Viviane Reding, pidiéndole que solicitara una aclaración al Gobierno estadounidense sobre el alcance de estos programas y sobre la afectación a ciudadanos europeos. Se envió también una segunda carta, en el mes de agosto, con mayores detalles sobre la valoración preliminar que el Grupo hacía del caso a partir de la limitada y heterogénea información disponible.

Posteriormente, el Presidente del GT29 fue designado por la Comisión para participar en el Grupo de Expertos conjunto UE-EEUU encargado de analizar el tema. Igualmente, el Presidente fue invitado a expresar la posición de las Autoridades de Protección de Datos en una audiencia pública enmarcada en la investigación formal que la Comisión LIBE del Parlamento Europeo ha llevado a cabo.

En paralelo, varios subgrupos de trabajo del GT29 han estudiado las implicaciones de estos programas, obviamente desde la perspectiva de la protección de datos, pero centrándose separadamente en su posible encaje en la legalidad europea, sus efectos sobre otros programas existentes en materia de seguridad (como el relativo a datos PNR o el TFTP II) y también sobre los instrumentos de transferencias internacionales.

En este contexto, el GT29 está prestando especial atención al funcionamiento de los mecanismos de transferencia internacional de datos entre la Unión Europea y los Estados Unidos que fundamentalmente se articulan sobre el sistema conocido como Safe Harbor o Puerto Seguro y que, según los resultados de la evaluación realizada por la Comisión Europea publicada en noviembre de 2013, presenta notables debilidades. La propia Comisión ha formulado hasta trece recomendaciones para revisar el Safe Harbor y ha iniciado negociaciones con la contraparte norteamericana con el fin de que antes del verano de 2014 se pueda alcanzar un acuerdo sobre las posibles soluciones a las debilidades detectadas.

A partir de estos análisis, y ya fuera del marco temporal que concierne a esta Memoria, el Grupo ha publicado una Opinión a este respecto. (Opinión 4/2014)

C - UNA POLÍTICA COORDINADA EN DEFENSA DE LOS CIUDADANOS EUROPEOS

El Grupo de Autoridades Europeas de Protección de Datos (GT29) siguió durante 2013 con la investigación coordinada que se inició en febrero de 2012 en relación con la nueva política de privacidad de Google.

Google introdujo esta política el 1 de marzo de 2012 y, como se describió en la anterior Memoria, la primera fase de investigación conjunta de las Autoridades Europeas concluyó con el envío a Google de un informe con los resultados de esa investigación y una carta en la que se formulaban una serie de recomendaciones orientadas a alinear la nueva política de privacidad con la normativa europea.

Ante la falta de respuesta de Google, el Grupo de Autoridades acordó en febrero de 2013 iniciar acciones en el plano nacional y que las actuaciones que pudieran desarrollar las Autoridades con competencias suficientes o mejor situadas para abrir procedimientos en esta línea se llevaran a cabo de forma coordinada, creándose una *task-force* liderada por la CNIL francesa. En esa *task force* se ha integrado la Agencia Española de Protección de Datos junto con las Autoridades de Alemania, Holanda, Italia y Reino Unido.

En el marco de la coordinación entre estas Autoridades, el día 2 de abril de 2013 comenzaron los procedimientos que, dentro de sus respectivos marcos legales, permiten realizar actividades de inspección a un responsable como paso previo a eventuales acciones sancionadoras. En el caso de la AEPD, se acordó el inicio de actuaciones previas de investigación. Posteriormente, el 20 de junio, todas las Autoridades pasaron a las segundas etapas de sus respectivos procedimientos. En España ese paso consistió en la apertura de un procedimiento sancionador a la vista de que de las actuaciones previas se desprendían indicios de la posible comisión de una serie de infracciones de la Ley Orgánica de Protección de Datos.

La Autoridad holandesa fue la primera en entrar en la fase final de su procedimiento, haciendo público su Informe final el 28 de noviembre de 2013. Este informe concluye que la nueva política de privacidad y la unificación de servicios vulneran la legislación holandesa en varios aspectos.

El procedimiento iniciado por la Agencia Española de Protección de Datos concluyó el 19 de diciembre de 2013 con una resolución en la que se constata el incumplimiento por parte de Google de varios preceptos de la legislación española relativos a información, ejercicio de derechos y legitimidad del tratamiento, que suponen tres infracciones graves de la LOPD.

La Autoridad francesa, por su parte, emitió su decisión final, en la que también se declaran varias infracciones similares a las identificadas en las decisiones holandesa y española, en los primeros días de 2014; imponiendo la máxima sanción que permite su ordenamiento y ordenando publicar la resolución durante 48 horas en la página principal del buscador. El resto de Autoridades actuantes continúan tramitando sus procedimientos.

En la Resolución de la Agencia (PS/00345/2013) se constata que Google recoge y trata ilegítimamente información personal, tanto de los usuarios autenticados (dados de alta en sus servicios) como de los no autenticados, e incluso de quienes

son meros usuarios pasivos, que no han solicitado sus servicios pero acceden a páginas que incluyen elementos gestionados por la compañía sin explicitarlo.

Google recopila información personal a través de casi un centenar de servicios y productos que ofrece en España sin proporcionar en muchos casos una información adecuada sobre qué datos se recogen, para qué fines se utilizan y sin obtener un consentimiento válido de sus titulares. En particular, no se informa con claridad a los usuarios de Gmail de que se realiza un filtrado del contenido del correo y de los ficheros anexos para insertar publicidad. Además, cuando se informa, se utiliza una terminología imprecisa, con expresiones genéricas y poco claras que impiden a los usuarios conocer el significado real de lo que se plantea.

La falta de información adecuada, particularmente sobre las finalidades específicas que justifican el tratamiento de los datos, impide que pueda considerarse que existe un consentimiento específico e informado y, en consecuencia, válido.

Por otra parte, Google combina la información personal obtenida a través de los diversos servicios o productos para utilizarla con múltiples finalidades que no se determinan con claridad, vulnerando con ello la prohibición de utilizar los datos que se recogen en un servicio con los obtenidos en otros. Esta combinación de los documentos que permite a Google enriquecer la información personal que almacena excede ampliamente las expectativas razonables del usuario medio, que no es consciente del carácter masivo y transversal del tratamiento de sus datos.

A ello hay que sumar que Google almacena y conserva datos personales por periodos de tiempo indeterminados o injustificados, contraviniendo con ello el mandato legal de proceder a su cancelación cuando dejan de ser necesarios para la finalidad que determinó su recogida.

Finalmente, la Resolución concluye que Google obstaculiza –y en algunos casos impide– el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El procedimiento que los ciudadanos deben seguir para ejercer sus derechos o gestionar su propia información personal les obliga a recorrer un número indeterminado de páginas, dispersas o en varios enlaces, que no están disponibles para todos los tipos de usuarios y, en ocasiones, con denominaciones que no siempre hacen referencia a su objeto. La propia compañía reconoce que hay que ejecutar al menos siete procesos diferentes, reservándose incluso el derecho de no atender las solicitudes que supongan «un esfuerzo desproporcionado».

La resolución de la AEPD declara, en consecuencia, la existencia de tres infracciones graves de la Ley Orgánica de Protección de Datos, imponiendo a Google una sanción de 300.000 euros por cada una de ellas e instando a la compañía a adoptar las medidas necesarias para adaptar su actividad a la normativa española.

D - LA MONITORIZACIÓN DE LA CONDUCTA DE LOS USUARIOS EN INTERNET (COOKIES)

El uso de dispositivos de almacenamiento y recuperación de información en los equipos terminales de los usuarios, cuya manifestación más conocida son las denominadas cookies, se ha generalizado en los servicios de internet.

La modificación del sistema de garantías de los usuarios ha pasado de un régimen basado en el derecho a obtener información sobre las cookies y disponer de un derecho de oposición (*opt-out*) a una exigencia de obtener su consentimiento informado *(opt-in)* establecido por el Real Decreto-ley 13/2012 de 30 de marzo. Ante las múltiples implicaciones de este cambio, la AEPD puso en marcha una iniciativa de colaboración con los representantes de la industria para elaborar unas orientaciones que facilitaran el cumplimiento efectivo del nuevo marco normativo.

Esta iniciativa concluyó con la presentación en abril de 2013 de la *Guía sobre el uso de las cookies*, la primera en el ámbito europeo elaborada conjuntamente por una Autoridad de Protección de Datos y los representantes de los sujetos obligados.

Conscientes de que el cambio normativo puede producir un fuerte impacto en amplios sectores de internet cuyo modelo de negocio descansa, total o parcialmente, en los ingresos derivados de la llamada publicidad personalizada —basada en el análisis de los intereses, gustos o preferencias asociadas a la navegación de los usuarios—, la Guía ofrece fórmulas flexibles que facilitan una aproximación progresiva para el cumplimiento de la nueva regulación, adaptable a los distintos modelos de negocio en internet.

La Guía describe los distintos tipos de cookies partiendo de la incidencia que tienen en la protección de los usuarios. Para ello se tiene en cuenta quién gestiona las cookies, distinguiendo si son propias del editor o de terceros, ya que habrá que obtener un consentimiento informado para unas y otras; así como el período de activación (cookies de sesión o persistentes), por la menor o mayor intrusión que implican para la navegación del usuario. Además se describen las finalidades del uso de las cookies, ya que la obtención del consentimiento informado debe partir del conocimiento por parte del usuario de la finalidad para la que se utilizarán. Recogiendo los criterios del conjunto de Autoridades de Protección de Datos de la Unión Europea, en el Dictamen 4/2012, se indican las cookies que estás exentas de las obligaciones de informar y obtener el consentimiento.

Sobre estas premisas, la Guía recomienda llevar a cabo una revisión de las cookies que se instalan en el sitio web con el fin de incorporar las cláusulas informativas que han de incluirse y las modalidades de obtención del consentimiento.

La obtención de un consentimiento informado constituye el eje de la regulación sobre cookies, por lo que la guía señala que es preciso potenciar la accesibilidad y visibilidad de las clausulas informativas, adaptándolas a las características del modelo de negocio del editor. Para facilitar cómo informar a los usuarios se admite la opción de suministrar la información por capas, de forma que en una primera capa se ofrezca al usuario la información básica en el momento en que accede al sitio web, enlazando con una segunda capa en la que se complementa la información de forma detallada.

La obtención del consentimiento admite, también, fórmulas flexibles que comprenden desde consentimientos expresos a través de un clic del usuario hasta consentimientos inferidos de una conducta que éste realice, como puede ser el continuar navegando en la web. En todo caso, han de ofrecerse procedimientos sencillos para que el usuario pueda desactivar las cookies o revocar el consentimiento. De este modo, las orientaciones recogidas en la Guía ofrecen diferentes fórmulas para la obtención del consentimiento informado con objeto de faci-

litar el cumplimiento de la nueva regulación atendiendo a las necesidades de cada editor.

La prioridad de la Agencia en la elaboración de esta iniciativa de carácter preventivo no condiciona el cumplimiento de la obligación legal de dar trámite a las denuncias presentadas por presuntos incumplimientos legales, circunstancia que ha dado lugar al inicio de actuaciones de inspección y a la tramitación de procedimientos sancionadores por incumplimiento del artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

Durante 2013 se han abierto 19 expedientes de actuaciones de investigación como consecuencia de denuncias presentadas ante la Agencia, y se han iniciado dos procedimientos sancionadores por no cumplir los requisitos de información sobre cookies, en primer lugar, en las páginas web de un grupo de empresas y, en segundo término, a Google Inc por falta de información sobre el almacenamiento y uso de cookies en los terminales de los usuarios que acceden a los blogs creados a través de la plataforma Blogspot.

El primero de los procedimientos concluyó en enero de 2014 (PS/00321/2013). La resolución de este procedimiento parte de la omisión, constatada al iniciarse las actuaciones de inspección, de la obligación de informar. No obstante, a la vista de las iniciativas adoptadas por los editores de los sitios web durante la tramitación del procedimiento para informar a los usuarios, se analiza su adecuación a las exigencias legales facilitando nuevos criterios orientadores sobre cómo cumplirlas.

La declaración de la infracción cometida se limita al incumplimiento del deber de información excluyendo la relacionada con la obtención del consentimiento al no estar adecuadamente tipificada esta última infracción en el artículo 38.8 g) de la LSSI. Es necesario mencionar que esta omisión fue corregida en el Proyecto de Ley de Telecomunicaciones que inició su tramitación parlamentaria en 2013 y se aprobó en mayo de 2014, fuera del espacio temporal recogido por esta Memoria.

Las sanciones impuestas a los editores afectados oscilan entre los 500 y 3.000 euros, atendiendo en este último caso al hecho de ser titular de varios sititos web sin incluir cláusulas informativas en ninguno de ellos.

E - MODULAR LAS GARANTÍAS EN EL CLOUD COMPUTING

El vertiginoso desarrollo de servicios Cloud computing y la necesidad de ofrecer un criterio común sobre las garantías que debe ofrecer su contratación en el entorno europeo, dieron lugar a la adopción por parte de las Autoridades de Protección de Datos de la Unión Europea del Dictamen 5/2012, que ofrece unas indicaciones armonizadas sobre la contratación de estos servicios.

Partiendo de este documento y de las conclusiones de la consulta pública promovida por la AEPD, la Agencia asumió la iniciativa de analizar aspectos necesitados de clarificación o precisiones adicionales para su contratación en España. Estas actuaciones han concluido con la presentación pública de dos documentos dirigidos a facilitar el cumplimiento de la normativa de protección de datos tanto a los clientes interesados en su contratación como a los oferentes de tales servicios: La *Guía para clientes que contraten servicios de Cloud computing* y las *Orientaciones para prestadores de servicios de Cloud computing*.

Dada la amplitud del abanico de potenciales clientes de estos servicios —que comprenden desde autónomos y profesionales hasta grandes corporaciones y administraciones públicas, pasando por pequeñas y medianas empresas— estos documentos optan por un enfoque eminentemente práctico que, sin prescindir del rigor técnico, permiten conocer los distintos tipos de nube y las modalidades de prestación de estos servicios, así como los elementos de riesgo que han de tenerse en cuenta y las garantías exigibles para su contratación.

El núcleo central de la Guía lo configura el apartado titulado «lo que debe conocer para la contratación», en el que se recogen 12 preguntas básicas en esta materia con sus correspondientes respuestas. Con el fin de facilitar y completar la información sobre la contratación, las respuestas incluyen enlaces a través de los que puede obtenerse información adicional.

La Guía aclara la posición jurídica de quienes intervienen en la contratación de estos servicios, señalando que el cliente mantiene la posición de responsable del tratamiento y que el oferente de servicios de Cloud computing es un encargado del tratamiento. Lo que implica que, siendo la legislación aplicable a las prestaciones de servicios la del responsable que los contrata, las garantías exigibles son las establecidas en la normativa española de protección de datos personales.

En este sentido, se destaca que, dadas las características de los servicios de Cloud computing, ofertados principalmente por compañías norteamericanas, el cliente debe acentuar la diligencia exigible para obtener una información completa sobre los mismos. Partiendo de esta información, la selección del proveedor debe tener en cuenta no sólo las variables de precio y calidad del servicio sino también las garantías contractuales para la protección de los datos personales de los que es responsable.

Por otra parte, los criterios que tradicionalmente se han aplicado en las relaciones entre el responsable y el encargado del tratamiento deben modularse para adaptarlas a las características propias de este entorno tecnológico.

En este sentido, la *Guía para clientes que contraten servicios de Cloud computing* ofrece soluciones flexibles sobre cómo incorporar en los contratos garantías adaptadas a este nuevo paradigma, especialmente en lo relativo a la supervisión de la subcontratación por el responsable del tratamiento, las transferencias internacionales de datos y la auditoría de las medidas de seguridad. Y destaca como un aspecto prioritario la necesidad de incorporar en los contratos cláusulas que garanticen la portabilidad de la información al término de la prestación del servicio, de forma que el cliente pueda mantener un control efectivo sobre los datos personales de los que es responsable.

La Guía dedica un apartado específico a la contratación de estos servicios por parte de las Administraciones Públicas, señalando que son exigibles garantías adicionales para cumplir con las obligaciones de los Esquemas Nacionales de Seguridad e Interoperabilidad aprobados por los Reales Decretos 3/2010 y 4/2010, respectivamente.

Las *Orientaciones para prestadores de servicios de Cloud computing*, tomando en cuenta las especificidades que se han señalado y la posición de las corporaciones que los prestan, reitera la especial diligencia que les es exigible para informar de forma transparente a sus clientes, tanto sobre la naturaleza de sus servicios como sobre las garantías para

el cumplimiento de la normativa española de protección de datos personales recogidos en la Guía, a la que se remite el documento de orientaciones.

F - REFORZAR LA PROTECCIÓN DE DATOS DE LOS MENORES DE EDAD

El uso de las nuevas tecnologías de la información y la comunicación asociadas a internet por parte de los menores de edad, especialmente las redes sociales o las aplicaciones de mensajería instantánea, es prácticamente universal a partir de una edad cada vez más temprana.

Según la Comisión Europea[1], la edad media en la que se comienza a navegar por internet es de 7 años y, según un estudio monográfico de IAB[2], el 93% de los jóvenes entre 14 y 17 años es usuario de las redes sociales, lo que en la mayoría de los casos implica una utilización de los datos de carácter personal, tanto los propios de los menores usuarios de la Red como de terceros, pues para poder hacer uso de estos servicios es requisito previo registrarse con los datos personales.

Estamos ante una situación en la que los menores viven con naturalidad con y en la Red. Sin embargo, esa familiaridad con el mundo digital no excluye los riesgos que para la protección de los datos de carácter personal y la privacidad comporta un uso poco responsable de la propia información personal y de la de terceros. No en vano, muchas de las situaciones de riesgo son facilitadas o propiciadas por un uso poco consciente de la información personal.

Con la finalidad de educar y sensibilizar a la población más joven de la importancia de la privacidad y del valor que para esta tienen los datos de carácter personal, la Agencia ha creado el portal Tú decides en internet (www.tudecideseninternet.es), que se presentó el 24 de octubre de 2013 y que desde esa fecha y hasta el 31 de diciembre ha registrado cerca de 12.000 visitas.

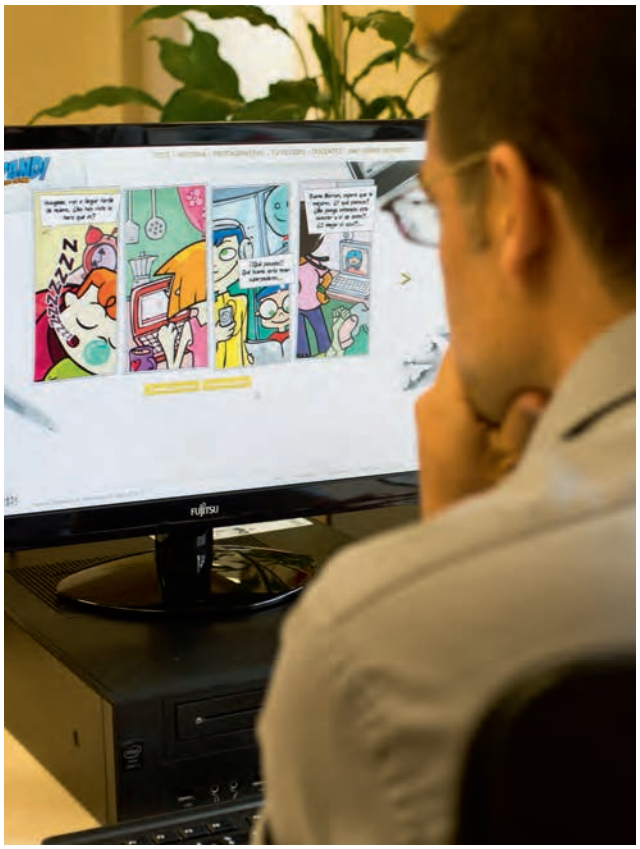
El portal proporciona una plataforma de consulta y apoyo especialmente orientada a la formación de los jóvenes entre 10 y 15 años, franja de edad que abarca desde los inicios en la Red hasta su uso intensivo. El portal comprende dos partes. Una de ellas está dirigida exclusivamente a los menores, más amena y en formato cómic, que plantea situaciones en las que la privacidad de los jóvenes se ve comprometida y ante las que se les pide que actúen, ofreciéndoles acto seguido la solución a las mismas. La segunda parte está dirigida fundamentalmente a educadores y padres. Incluye fichas didácticas que se pueden utilizar en clase y en las que se tratan en detalle los diferentes temas relacionados con el uso de internet por los menores, con recomendaciones y materiales de interés para aquellos que quieran ampliar la información sobre cada uno de los temas tratados.

El portal y sus contenidos quieren ser una herramienta útil para la formación de los menores y, de ese modo, contribuir a prevenir los riesgos que se pueden derivar de un mal uso o un uso inconsciente de algunos servicios de internet.

La LOPD establece que para poder prestar el consentimiento para el tratamiento de los datos de carácter personal se requiere la edad mínima de 14 años y que, en caso contrario, deben prestarlo los padres, tutores o representantes legales. En consecuencia, otro aspecto que es preciso reiterar es la

[1] Comunicación sobre una estrategia europea a favor de una internet más segura para los niños.

[2] Interactive Advertising Bureau: Asociación que representa al sector de la publicidad en medios digitales en España.



obligación por parte de los responsables del tratamiento de articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor.

La Agencia no es ajena a que esta obligación puede presentar dificultades prácticas a la hora de encontrar instrumentos eficaces que permitan llevar a cabo la comprobación de la edad de los menores en determinados servicios de internet, como las redes sociales.

Por ello, la Agencia mantiene reuniones periódicas con los principales responsables de las redes sociales para evaluar los avances en la comprobación de la edad.

Para contribuir a que estos dispongan de instrumentos que faciliten el cumplimiento de la obligación de verificar la edad de los menores, la Agencia propuso que el DNI de los menores llevase activado el certificado de autenticación, lo que se ha llevado a cabo mediante la modificación del Real Decreto, 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica, realizada por el Real Decreto 869/2013, de 8 de noviembre. Esta modificación implica que los DNI que se expidan a los menores de edad se van a emitir con el certificado de autenticación activado, permitiendo conocer la edad real del menor mediante la identificación electrónica y facilitando a los proveedores de servicios en internet el cumplimiento de esta obligación. Un ejemplo de ello es el caso de Tuenti, que implantó en abril de 2013 un sistema de verificación de la edad a través del DNI.

El compromiso de la Agencia con respecto a la utilización de datos personales de menores también tuvo reflejo en una comparecencia del director de la AEPD ante la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la red por parte de los menores, constituida en el seno de la Comisión conjunta de las Comisiones de Interior, de Educación y Deporte, y de Industria, Energía y Turismo del Senado.

G - USO DE APLICACIONES EN DISPOSITIVOS INTELIGENTES

La proliferación masiva de los teléfonos inteligentes y otros dispositivos como tabletas o televisores que permiten acceso a internet ha favorecido el desarrollo de un sinnúmero de aplicaciones de uso general o específico que trasciende el conjunto de prestaciones asociadas al uso y gestión tradicional de estos dispositivos.

3

España es el primer país de Europa tanto en usuarios de teléfonos como de aplicaciones inteligentes, con 23 y 22 millones de usuarios respectivamente, siguiendo datos de 2013. Con una media de entre 20 y 30 aplicaciones instaladas por dispositivo, dependiendo del tipo, estas apps representan el medio más habitual tanto para actividades de comunicación, incluyendo el correo electrónico, como para el acceso a redes sociales y a fuentes de información y entretenimiento, con un componente bastante elevado en servicios de localización.

Las Autoridades europeas de Protección de Datos decidieron abordar esta cuestión a través de un Dictamen sobre las aplicaciones de los dispositivos inteligentes (Dictamen 2/2013) adoptado el 27 de febrero, siendo la Agencia Española de Protección de Datos una de las ponentes.

El Dictamen identifica los principales riesgos para la protección de datos, haciendo particular hincapié en la falta de transparencia hacia los usuarios derivada de la falta de información o de la presencia de ésta de forma incompleta o poco clara en lo que se refiere a los tipos de datos tratados y a la finalidad de dicho tratamiento. Estrechamente relacionada con la falta de información se encuentra la dificultad para poder proporcionar el consentimiento al tratamiento de forma libre e informada. Esta situación se ve, además, agravada por la dificultad adicional de no poder matizar dicho consentimiento para tratamientos particulares dentro de la misma aplicación, sin que sea posible no otorgar, por ejemplo, el consentimiento para geolocalizar al dispositivo en una aplicación que no tiene ese servicio como finalidad principal, mientras que se consiente al resto de los tratamientos.

El incumplimiento del principio de limitación de la finalidad es otro de los riesgos claves asociados al uso de estas aplicaciones sin que se pueda dejar de citar, como uno de los riesgos cada vez más presentes en el ánimo del usuario, el relacionado con la ausencia, en muchos casos, de medidas de seguridad suficientes que impidan el acceso y tratamiento de datos por parte de terceros no autorizados.

El documento trata de identificar con precisión a los actores que forman parte del ecosistema de las aplicaciones inteligentes, prestando particular atención a los desarrolladores de dichas aplicaciones, a los fabricantes de dispositivos y sistemas operativos en los que se ejecutan y, no en menor medida, a las tiendas de aplicaciones, que son la interfaz principal de acceso del usuario al conjunto de aplicaciones disponibles para su dispositivo. Para todos ellos se definen una serie de obligaciones y recomendaciones cuyo objetivo fundamental es delimitar sus márgenes de actuación, a la vez que se ofrece un conjunto de buenas prácticas que tratan de facilitar que el usuario tenga plena disponibilidad y control sobre sobre sus propios datos personales.

Elementos clave de esas recomendaciones son la obligación de requerir el consentimiento de forma previa a que las aplicaciones comiencen a recopilar información personal o de que sean efectivamente instaladas en el dispositivo, así como solicitarlo de forma diferenciada o granular para cada tipo de datos que se pretende tratar.

El Dictamen especifica que la información debe ser clara y comprensible, muy en particular cuando los datos van a ser utilizados para fines relacionados con terceros, como pueden ser la publicidad o el análisis de información. De la misma forma, a los usuarios se les debe permitir revocar la autoriza-

ción en cualquier momento, así como garantizar que la desinstalación de la aplicación lleva aparejada la supresión efectiva de los datos. En este mismo ámbito, se advierte claramente sobre la necesidad de respetar el principio de minimización de datos tratando exclusivamente los necesarios para realizar la función deseada y limitando el periodo de retención de los mismos al estrictamente necesario para el cumplimiento de la finalidad para la que fueron recogidos.

Finalmente el documento reitera la necesidad de garantizar la seguridad adoptando las medidas técnicas y organizativas adecuadas en todas las fases de desarrollo de la aplicación, favoreciendo el uso de técnicas de privacidad por defecto y privacidad desde el diseño.

Las tiendas de aplicaciones, por su parte, son objeto de recomendaciones específicas, al ser el principal punto de contacto del usuario que, además, tiende a considerar que las aplicaciones ofrecidas para descarga han sido previamente validadas por los gestores de la tienda, garantizando así un plus de confianza en la bondad de las mismas y en el respeto a las normas sobre privacidad. En esa línea, se recomienda someter a todas las aplicaciones a un mecanismo de evaluación pública y a poner en marcha canales de información que permitan al usuario notificar problemas relacionados con la seguridad o con la protección de datos de carácter personal.

También se ofrecen recomendaciones a los fabricantes de dispositivos y sistemas operativos en el sentido de garantizar la seguridad y, muy en particular, que los métodos y funciones que permiten acceder a los datos de carácter personal incluyan medidas para aplicar el consentimiento granular y que este no pueda ser revocado de forma unilateral por las aplicaciones utilizando vías de acceso alternativas al sistema.

Por último, se hace una mención específica a los menores, que son usuarios de aplicaciones desde edad muy temprana. Partiendo de una referencia

general a las recomendaciones recogidas en el dictamen 2/2009 sobre la protección de los datos personales de los niños, se incluyen referencias específicas a la atención al límite de edad que define a los menores de edad en las legislaciones nacionales, lo que hace condición previa el consentimiento parental al tratamiento, así como a la necesidad de prestar atención a las posibles limitaciones de comprensión y atención de los menores a la hora de recibir información sobre el tratamiento de sus datos. El principio de minimización de datos y el de limitación de la finalidad se han de respetar de for-

ma aún más rigurosa en las aplicaciones dirigidas a menores, haciendo una muy especial referencia a la imposibilidad de tratar datos de niños con fines de publicidad comportamental por quedar fuera del ámbito de comprensión del niño y, de esa manera, exceder los límites del tratamiento lícito.

No hay duda de que el uso de aplicaciones inteligentes va a seguir creciendo, no solo en número, sino también en los ámbitos en los que van a ser de uso habitual. Esto no excluye que alguno de los riesgos descritos se multiplique y alcance ámbitos de actividad personal hasta ahora excluidos. Estas aplicaciones se están convirtiendo en la plataforma primordial del desarrollo de servicios integrados en la denominada Internet de las Cosas, a la vez que representan una fuente de gran interés para la recopilación de información que puede ser analizada con las técnicas utilizadas por el Big Data lo que, sin duda, va a contribuir a que este fenómeno siga recibiendo atención por parte de las Autoridades de Protección de Datos.

H - LOS FLUJOS INTERNACIONALES DE DATOS: FLEXIBILIDAD Y GLOBALIZACIÓN

Los flujos internacionales de datos en un mundo globalizado mantienen su tendencia creciente con un total de 170 autorizaciones por parte de la Agencia Española de Protección de Datos en 2013.

Los países latinoamericanos siguen ocupando el primer lugar como importadores de datos desde España, seguidos de EEUU. Sin embargo, es preciso destacar el incremento de transferencias internacionales de datos con destino a India, que en un año casi se han duplicado (42 frente a 27) ascendiendo a un total de 179. Estos datos ponen de manifiesto una tendencia a la diversificación de los países de destino de los flujos internacionales de datos exportados, y contribuyen a justificar el creciente interés de dicho país para encontrar vías que faciliten las transferencias internacionales de datos desde la Unión Europea.

La gran mayoría de las transferencias internacionales (72%) tienen como objeto la prestación de servicios por parte de entidades ubicadas en terceros países (encargados del tratamiento), lo que indica la importancia que está adquiriendo la deslocalización de servicios en el actual entorno tecnológico.

La necesidad de aportar modelos flexibles para transferir datos a terceros países se ha puesto de manifiesto en la presentación de 10 solicitudes de autorización (nueve finalizadas y concedidas en 2013) basadas en las garantías proporcionadas por las denominadas Reglas Corporativas Vinculantes (BCR, por sus siglas en inglés), así como en la de siete solicitudes amparadas en el modelo de garantías desarrollado por la AEPD para facilitar las transferencias internacionales en las que los exportadores de datos son encargados del tratamiento establecidos en España que subcontratan con entidades ubicadas en terceros países para la prestación de servicios.

La utilidad de este modelo de autorizaciones basadas en un contrato marco ha quedado acreditada en 2013, año en el que ascienden a 454 (con 1.561 ficheros afectados) los responsables del tratamiento de datos que han suscrito un contrato para la prestación de servicios con un encargado que previamente había obtenido una autorización para la transferencia internacional de datos como exportador a un subencargado del tratamiento.

El citado modelo ha permitido que las entidades responsables del tratamiento de datos se hayan beneficiado de dichas autorizaciones marco con la simple notificación de la transferencia al Registro General de Protección de Datos, sin necesidad de solicitar

la correspondiente autorización caso por caso, con el consiguiente ahorro de tiempo y costes para el cumplimiento de sus obligaciones legales.

Adicionalmente, la AEPD ha contribuido a facilitar las transferencias internacionales desde la Unión Europea participando, a través del procedimiento coordinado establecido por el Grupo de Autoridades europeas de Protección de Datos (GT29), en la revisión de tres solicitudes de aprobación de BCR's presentadas ante las Autoridades de Protección de Datos de Francia y Reino Unido.

La importancia de la contratación de prestadores de servicios en terceros países, unida a la necesidad de desarrollar fórmulas flexibles para los flujos internacionales de datos, se ha traducido en el impulso de las denominadas BCR para encargados del tratamiento, que pretenden ser de aplicación para las entidades pertenecientes a un grupo multinacional que actúe como prestador de servicios. Estos trabajos se han desarrollado en el subgrupo BCR del GT29 contando con la participación activa de la Agencia Española.

4 MARCOS SUPRANACIONALES DE PROTECCIÓN DE DATOS

A - AVANCES EN LA REVISIÓN DE LOS MARCOS INTERNACIONALES

En 2013 han continuado los procesos de actualización y modernización de algunos de los principales instrumentos internacionales de protección de datos que se iniciaron en años anteriores.

El 25 de enero de 2012 la Comisión Europea presentó sus propuestas de Reglamento General sobre Protección de Datos y de Directiva sobre protección de datos en el ámbito policial y judicial penal.

En el Consejo, y bajo las Presidencias irlandesa y lituana, continuaron los trabajos sobre la propuesta de Reglamento en el seno del Grupo DAPIX. Aunque ambas Presidencias mantuvieron un intenso ritmo de actividad, no ha sido posible alcanzar una posición común ni tampoco cerrar acuerdos sobre partes completas del texto.

Por su parte, en el Parlamento la Comisión LIBE votaba el 21 de octubre de 2013 sendas posiciones comunes sobre el Reglamento y la Directiva. En el caso concreto del Reglamento, es obligado reconocer el importante esfuerzo realizado para llegar a este punto, dado que ha sido necesario procesar las más de 3.000 enmiendas presentadas al texto, una tarea que obligó a retrasar la votación en varias ocasiones desde la primera fecha prevista, en abril de 2013.

Los diferentes ritmos seguidos por Parlamento y Consejo han conducido a que a principios de 2014 se hiciera evidente que resultaría extremadamente difícil que pudiera aprobarse un texto definitivo de Reglamento antes del fin de la celebración de elecciones para la renovación del Parlamento Europeo, a celebrar el 25 de mayo de 2014, así como de la elección de una nueva Comisión siguiendo los criterios establecidos por el Tratado de Lisboa. En esos momentos, todo parecía indicar que un escenario razonable sobre la marcha de las negociaciones podría consistir en que el Consejo alcanzara una posición común a lo largo de 2014, de forma que pudieran iniciarse los *trílogos*, discusiones a tres bandas con Parlamento Europeo y Comisión, y lograr la aprobación definitiva a principios de 2015.

La propuesta de Directiva ha sido también estudiada por el Grupo DAPIX, si bien con una menor dedicación que en el caso del Reglamento. Este ritmo más pausado se impuso ya desde los primeros compases de la negociación en 2012 y parece ser fruto de una variedad de factores. Entre ellos se encuentran las dudas de varios Estados miembros sobre la necesidad de adoptar esta norma cuando aún no se ha podido evaluar el impacto de la Decisión Marco de 2008 o también el rechazo de las sucesivas presidencias a complicar aún más las ya de por sí complejas discusiones sobre el Reglamento.

En cualquier caso, el hecho es que el Grupo prosigue su estudio del documento sin que hasta el momento se haya presentado ninguna propuesta de acuerdo o conclusión al Consejo.

Esta situación contrasta con la ya descrita en el Parlamento Europeo, donde, en la misma línea defendida por la Comisión, se ha impuesto la conocida como «aproximación integral» a las propuestas de revisión, lo que supone que el Reglamento y la Directiva fueron estudiados en paralelo y que la adopción de los informes en la Comisión LIBE se produjo también simultáneamente.

La Agencia Española de Protección de Datos, como órgano independiente de la Administración del Estado, no asume la representación española en las discusiones que sobre este nuevo marco normativo se desarrollan en el Consejo ni, obviamente, en el Parlamento Europeo. No obstante, está participan-

<Índice>

do activamente a título consultivo prestando asesoramiento y asistencia de contenido fundamentalmente técnico a los Departamentos responsables en el marco de los mecanismos de coordinación que se han establecido específicamente para abordar la tramitación de este paquete normativo.

La AEPD ha participado también activamente en la preparación de las reacciones del GT29 a estas iniciativas normativas. En concreto, la Agencia ha tomado parte en todas las reuniones del Grupo y de su Subgrupo Futuro de la Privacidad, en que se han preparado documentos relacionados con el proceso de revisión, y ha participado en la preparación de todas las Opiniones que el Grupo ha emitido y que se relacionan en el apartado correspondiente de esta Memoria.

Por otro lado, aunque su impacto directo en el derecho español de protección de datos pueda ser menor, no puede obviarse la importancia del segundo de los instrumentos que se encuentra actualmente en proceso de revisión. Se trata del Convenio 108 del Consejo de Europa, cuya reforma se abordó al tiempo de cumplirse los 30 años de su adopción en 1981.

La revisión del Convenio se lanzó formalmente por el Comité de Ministros a finales de 2010. El Comité Consultivo del Convenio trabajó durante 2011 y 2012 en la preparación de un documento técnico de propuesta de reforma y tras su última reunión plenaria, celebrada entre los días 27 y 30 de noviembre de 2012, remitió al Comité de Ministros la propuesta definitiva de texto articulado

Con esta remisión se iniciaba una nueva fase en el proceso de modernización del Convenio, en la cual un comité ad hoc (CAHDATA), en el que está presente la Presidencia del Comité Consultivo, ha de estudiar el texto siguiendo un mandato que emite el Comité de Ministros a propuesta del Standing Committee on Media and Information Society. Este Comité ad hoc celebró su primera reunión en noviembre de 2013.

En la anterior Memoria se hacía referencia a una cuestión que es una constante desde el inicio del proceso. Se trata de la necesidad de que exista coherencia entre el nuevo texto del Convenio y el marco de protección de datos revisado de la Unión Europea.

La consecución de ese objetivo está condicionada por dos factores. Por un lado, por la presentación de las propuestas de Reglamento y Directiva por parte de la Comisión en enero de 2012. Por otro lado, la Comisión Europea había manifestado expresamente su posición de que la política de protección de datos es de exclusiva competencia europea según el Tratado de Lisboa y que, por tanto, corresponde a las instituciones europeas negociar y concluir cualquier acuerdo internacional, incluido el nuevo Convenio, que regule la materia.

Ambas circunstancias persisten en el momento en que se cierra esta Memoria, pero con distintos matices. Respecto a la necesidad de mantener la coherencia entre la Convención y el acervo europeo en protección de datos, el principal obstáculo es que este acervo está en proceso de cambio y es necesario una constante valoración de los tres posibles textos de referencia: la Directiva 95/46, las propuestas de la Comisión y los sucesivos documentos de trabajo adoptados por el Consejo y el Parlamento, que apuntan a que el texto final no coincidirá necesariamente con el presentado por la Comisión.

La segunda de las cuestiones apuntadas se resolvió, al menos formalmente, cuando el Consejo, a resultas de una petición presentada por la Comisión en

noviembre de 2012, le concedió el mandato para negociar en el seno del CAHDATA (07/06/2013).

B - LA ACTIVIDAD DEL GRUPO DE TRABAJO DEL ARTÍCULO 29

El Grupo de Trabajo del Artículo 29 (GT29), creado por la Directiva 95/46/CE, tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que realiza funciones de secretariado. La Agencia Española de Protección de Datos forma parte del mismo desde su constitución en febrero de 1997.

En 2013 el GT29 celebró cinco reuniones plenarias y, aunque con menor intensidad que en el año anterior, siguió dirigiendo parte de su actividad a coordinar y preparar las aportaciones colectivas de las Autoridades de Protección de Datos al proceso de revisión del marco europeo de protección de datos. Asimismo, ha adoptado otros dictámenes y un documento sobre cuestiones relevantes para la protección de los datos personales.

■ Documentos sobre la revisión del marco europeo de protección de datos

En relación con las iniciativas de revisión del marco legal en la UE, el GT29 ha adoptado dos nuevos documentos (WP200 y WP201) en cuya elaboración la Agencia ha tenido un papel destacado.

El primero de ellos es, de hecho, complementario de uno de los capítulos del Dictamen 8/2012, que estaba dedicado al análisis de las habilitaciones a la Comisión para adoptar actos delegados que contiene la propuesta de Reglamento. El Documento de Trabajo de 2013 sigue en la misma línea, pero en relación con los actos de aplicación. El Documento mantiene los criterios de valoración ya fijados en el anterior Dictamen, es decir, el que la materia afectada por la habilitación se refiera o no a una parte esencial de la regulación del derecho, el que se trate o no de una materia que debe necesariamente regularse a dicho nivel, o si la cuestión debe tener un carácter legalmente vinculante o puede ser abordada mediante un instrumento más flexible.

El Documento WP201 es el primer texto aprobado por el Grupo en que, de manera separada, se aborda

la propuesta de Directiva en los ámbitos de policía y justicia penal. Ya en la primera reacción del GT29 al paquete de reforma, el Dictamen 1/2012, se incluía una segunda parte dedicada a la Directiva, pero esta propuesta no había vuelto a ser considerada por el Grupo. Una de las razones que explicarían este aparente desinterés estaría en que la mayor rapidez con que se han desarrollado las negociaciones sobre el Reglamento ha forzado al Grupo a reaccionar buscando posiciones comunes sobre temas clave de cara a intentar influir en las discusiones.

Este Documento se centra en cuatro elementos de la Directiva que, a juicio del Grupo, no están siendo adecuadamente tratados en la negociación en curso:

- Tratamientos de datos de personas no sospechosas
- Derechos de los interesados
- Evaluaciones de Impacto de Protección de Datos
- Poderes de las autoridades de supervisión

Junto con los anteriores documentos, a lo largo de las negociaciones en el Parlamento Europeo y en el Consejo han ido surgiendo cuestiones que, como se ha señalado en el apartado anterior, han movido al Grupo a reaccionar utilizando para ello los instrumentos formales que mejor se adaptan a las circunstancias de cada caso.

El primero de los documentos de este tipo es la Declaración sobre las actuales discusiones sobre la reforma en materia de protección de datos, publicado el 27 de febrero de 2013.

La declaración tiene dos partes diferenciadas. En la primera, el Grupo pasa revista a diversos temas centrales dentro de la propuesta del Reglamento en los que, a su juicio, la marcha de las negociaciones podría conducir a una disminución del nivel de protección existente o del que el Reglamento propone. Esas cuestiones se refieren, entre otras, a la idea de introducir modificaciones adicionales en el Reglamento para dar mayor flexibilidad a los tratamientos desarrollados por el sector público o el uso de los conceptos de seudonimización y anonimización.

La segunda parte de la Declaración la constituyen sendos Anexos monográficos sobre «Competencia y Autoridad Líder» y sobre «Excepción doméstica».

El Anexo sobre competencia y autoridad líder es la contribución del Grupo al debate que ha suscitado la propuesta del Reglamento sobre «ventanilla única». El Grupo ya había tratado el tema en el Dictamen de marzo de 2012 pero, en este caso, aparte de indicar una serie de principios básicos sobre cómo debería fijarse, a su juicio, la cooperación y coordinación entre Autoridades en la Unión, hace propuestas concretas sobre el articulado.

El acuerdo sobre este tema no fue fácil, dado que los miembros del Grupo tienen diferentes sensibilidades sobre la cuestión, derivadas, entre otras cosas, de sus normas internas sobre gestión de reclamaciones, de que cuenten o no con capacidad sancionadora o de que pertenezcan a Estados miembros con mayor o menor presencia de las sedes principales de compañías multinacionales. Por ello conviene señalar que el Anexo recoge puntos en que puede considerarse que hay un acuerdo de principio entre todas las Autoridades, sin perjuicio de que cada una de ellas pueda hacer diferentes interpretaciones de su contenido, condicionarlo al modo en que finalmente se regulen otras cuestiones o defender la inclusión de otros requisitos o procedimientos.

El segundo de los Anexos, sobre excepción doméstica, analiza las dificultades que internet y los

servicios de la sociedad de la información plantean a la hora de definir qué tipo de actividades de tratamiento de datos pueden considerarse incluidas en la esfera de lo puramente personal o doméstico.

Otro Documento adoptado por el Grupo en este mismo marco es el «Advise Paper», que fue publicado el 13 de mayo de 2013 y trata sobre elementos esenciales para una definición de perfilado, y una disposición reguladora del mismo.

Tras la adopción por la Comisión LIBE de su posición común, el GT29 reaccionó a través de dos documentos:

- El primero de ellos fue una Declaración en la que el Grupo mostraba su favorable acogida a la posición del Parlamento, al tiempo que expresaba su preocupación por el retraso en los trabajos y urgía a todos los actores implicados a intensificar su actividad para llegar a aprobar un texto durante el actual mandato del PE, desde el convencimiento de que es urgente adoptar un nuevo marco legal que asegure un elevado nivel de protección a los ciudadanos.

- El segundo de los textos que componen la reacción del Grupo es una carta, dirigida al Consejo, a la Comisión LIBE y a la Comisión, en la que se pone de relieve el acuerdo general con los términos de la posición alcanzada por la LIBE al tiempo que se identifican una serie de aspectos en los que el Grupo entiende que la posición puede ser mejorada o debe ser revisada.

- **Dictamen sobre limitación de finalidad (WP203)**

Este Dictamen analiza la limitación de finalidad como garantía para el interesado. Este principio fija los límites sobre cómo los responsables pueden tratar datos, al tiempo que ofrece cierto grado de flexibilidad permitiendo el uso para fines compatibles.

El Dictamen se extiende en analizar cómo la compatibilidad o incompatibilidad deben valorarse caso por caso, tomando en cuenta todas las circunstancias relevantes. En particular, son claves los siguientes factores:

- La relación entre la o las finalidades para las que los datos fueron recogidos y las finalidades de tratamientos ulteriores.

- El contexto en el que se recogieron los datos y las expectativas que razonablemente puede albergar el interesado sobre sus usos futuros.

- La naturaleza de los datos personales y el impacto de tratamientos ulteriores sobre los interesados.

- Las garantías adoptadas por el responsable para asegurar un tratamiento equitativo y para prevenir efectos indebidos sobre los interesados.

El Dictamen concluye que el tratamiento de datos personales de forma incompatible con las finalidades originalmente especificadas es ilegal y no puede ser legitimado simplemente mediante el recurso a otra de las bases legales previstas en el artículo 7 de la Directiva 95/46. Las restricciones al principio de limitación de finalidad solo pueden producirse a través de los mecanismos y con las condiciones previstas en el artículo 13 de la Directiva.

Esta conclusión es relevante también de cara al proceso de revisión del marco legal europeo, ya que la propuesta de Reglamento, al tiempo que mantiene el principio de limitación de finalidad, añade una

disposición según la cual los datos podrán tratarse para fines no compatibles siempre que pueda invocarse otra base legal, con la excepción del interés legítimo del responsable.

- **Dictamen sobre *Smart Borders* (WP206)**

El Dictamen se refiere al paquete legislativo que la Comisión presentó en febrero de 2013 para aplicar el llamado Programa Smart Borders. Incluye propuestas sobre un Sistema de Entrada y Salida (EES), sobre un Programa de Viajeros Registrados (RTP) para el Area Schengen y sobre diversas modificaciones del Código de Fronteras de Schengen.

El Dictamen se centra principalmente en la propuesta sobre el EES, que supone la existencia de un sistema de almacenamiento centralizado para datos de entrada y salida de nacionales de terceros países que han sido admitidos en el espacio Schengen para estancias de corta duración, se les haya o no exigido visa Schengen.

El Dictamen cuestiona que el Sistema de Entrada y Salida pueda resultar eficaz para alcanzar los objetivos que él mismo se marca. Se añade, además, que aunque el sistema ofreciera un valor añadido significativo, ese valor añadido no satisfaría un nivel de necesidad tal que pudiera hacer aceptable la interferencia con los derechos de acuerdo con el artículo 8 de la Carta de la Unión Europea. Al mismo tiempo, el Dictamen considera que ese valor añadido tampoco es proporcional a la intensidad del impacto sobre los derechos fundamentales en relación con cada uno de sus objetivos, teniendo en cuenta que hay otras alternativas para conseguir las metas fijadas.

En una segunda parte, el Dictamen enumera algunas implicaciones en materia de protección de datos de las otras dos propuestas que integran el Programa.

- **Dictamen sobre reutilización de información del sector público y *open data* (WP207)**

El GT29 acordó preparar este Dictamen, que actualiza otro de 2003, en el contexto de la discusión de la propuesta de la Comisión para modificar la vigente Directiva 2003/98 sobre reutilización de información del sector público.

El Grupo reitera su opinión de que la reutilización de la información del sector público puede producir beneficios en términos de mayor transparencia y de apertura de formas innovadoras de uso. Sin embargo, también subraya que la mayor accesibilidad de la información no está exenta de riesgos para los individuos, y que es por ello necesario mantener un equilibrio a la hora de decidir qué datos personales pueden o no ofrecerse para su reutilización y qué medidas deben adoptarse para salvaguardar los intereses de sus titulares.

En principio, el Dictamen considera que la reutilización no siempre es apropiada en los casos en que la información del sector público que va a ser reutilizada contiene datos personales. Frecuentemente, más que datos personales son datos estadísticos derivados de los datos personales los que se ponen a disposición del público y así debería seguirse haciendo.

Sin embargo, puede ser posible que en algunas situaciones los datos personales se consideren susceptibles de reutilización según la Directiva, si bien de acuerdo con medidas adicionales de carácter legal, técnico u organizativo destinadas a proteger a las personas afectadas. Es importante en estos casos que se establezca una base legal clara para poner a disposición pública los datos personales, tomando en consideración principios como el de proporcionalidad, minimización de datos y limitación de finalidad.

<Índice>

■ Documento de trabajo de guía sobre obtención del consentimiento para cookies (WP208)

Este Documento de Trabajo (2/2013) es la continuación de los dictámenes del Grupo sobre publicidad conductual sobre la Recomendación de Buenas Prácticas IAB/EASA y sobre cookies exentas de consentimiento en el marco de la aplicación de la Directiva de ePrivacy.

En este caso, y ante las diferencias existentes en las trasposiciones nacionales del artículo 5.3 de la Directiva de ePrivacy, el Grupo ha buscado identificar los criterios que permitirían a una empresa establecer mecanismos de obtención del consentimiento para el uso de cookies que aseguraran el cumplimiento de todas las legislaciones adoptadas en la Unión Europea, incluidas las que fijan requisitos más restrictivos. Evidentemente, y desde esa perspectiva, el Documento no pretende sustituir ni cuestionar lo que hayan podido determinar las legislaciones nacionales ni tampoco la aplicación que de esas legislaciones puedan hacer las respectivas Autoridades de Protección de Datos.

■ Carta sobre datos API

Como continuación de las discusiones que venía manteniendo con la Comisión en relación con el tratamiento y transferencia a terceros países de datos API (Advanced Passenger Information), el GT29 decidió elaborar un dictamen sobre este tema.

Los datos API son un conjunto reducido de datos personales (normalmente los incluidos en la parte legible mecánicamente de un pasaporte) que las líneas aéreas están obligadas, en aplicación de la legislación de terceros países, a transferir con anterioridad a la salida de vuelos dirigidos a tales países, procedentes de ellos o, en algunos casos, que los sobrevuelan. Más de 40 países solicitan tales datos o están preparándose para hacerlo. En los trabajos preparatorios se constató que existe una gran divergencia en la interpretación que Estados miembros y Autoridades de Protección de Datos hacen sobre la fundamentación legal para el tratamiento y transferencia de estos datos. Por ello, se decidió que en lugar de redactar un Dictamen sería más adecuado expresar sus preocupaciones en una carta a la Comisión.

Esta carta fue enviada el 11 de julio a la Comisaria de Asuntos de Interior en la Comisión Europea Cecilia Malmström. En ella, el grupo se refería a la disparidad de interpretaciones existentes entre los Estados miembros y señalaba que la Convención de Chicago de 1944 sobre Aviación Civil Internacional (que prevé la obligación de entregar datos de pasajeros antes de la llegada, tránsito o salida con finalidades de control fronterizo) sólo podría constituir base legal suficiente a partir de una interpretación muy favorable y siempre que se cumplan también los requisitos previstos en los artículos 25 y 26 de la Directiva 95/46.

Por ello, se solicitaba a la Comisaria que la Comisión considerara la posibilidad de adoptar algún instrumento legal europeo que sirviera como base suficiente y común a toda la Unión para este tipo de transferencias.

C - ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL

El año 2013 destacó por una cargada agenda legislativa en este ámbito. Junto con el ya citado desarrollo legislativo de la futura Directiva se han presentado nuevas propuestas de Reglamento para Europol y Eurojust que, a la vez que introducen cambios en su ámbito de actividad, han generado gran debate en relación con el modelo de supervisión en protección de datos que ha de ser utilizado. Finalmente, fue aprobado el nuevo Reglamen-

to Eurodac, aunque el nuevo sistema en él previsto no será efectivo hasta el año 2015.

El año 2013 ha sido también el de la puesta en marcha de la segunda generación del Sistema de Información Schengen, el SIS II, así como de la paulatina consolidación y despliegue global del Sistema de Información de Visados. Igualmente han tenido importancia las discusiones sobre el impacto que las diversas iniciativas de terceros países dirigidas a requerir datos de viajeros –API y PNR– han tenido sobre el debate acerca de la necesidad de una norma europea en este ámbito.

Sistema de Información Schengen

El Sistema de Información Schengen de segunda generación, SIS II, comenzó a funcionar de forma efectiva el 9 de abril de 2013, con la consecuencia de la entrada en vigor de forma inmediata de la nueva base jurídica aplicable –Reglamento CE 1987/2006 y Decisión 2007/533/JAI–, incluyendo la puesta en marcha de un nuevo modelo de supervisión en el ámbito de la protección de datos, con reparto de competencias entre las Autoridades nacionales y el Supervisor Europeo de Protección de Datos, reforzado por la creación del Grupo de Supervisión Coordinada del SIS II, integrado por representantes de los Estados miembros y del Supervisor. Dicho grupo ha comenzado a funcionar a lo largo del año, centrando su actividad en la elaboración de las reglas de funcionamiento y la determinación de un programa de trabajo para los próximos años.

La puesta en marcha del sistema vino igualmente acompañada de una campaña informativa de alcance global que incluía información relativa a las disposiciones de protección de datos incluidas en la normativa, así como a la forma en la que pueden ser ejercidos los derechos reconocidos al titular de los datos.

Otro elemento de relevancia fue la difusión de información sobre una brecha de seguridad que afectó al punto nacional Schengen del Reino de Dinamarca en el año 2012, lo que provocó la reacción inmediata por parte de la Comisión Europea y los Estados miembros creando un comité encargado de evaluar de forma global la seguridad del Sistema de Información Schengen. Dicho comité, en el que participa la Agencia Española de Protección de Datos, no había elevado su informe definitivo a finales del año 2013.

Por último, es de interés señalar que la Agencia participó en la Evaluación Schengen del Reino Unido que tuvo lugar en el mes de octubre. Dicha evaluación se realizó con carácter previo a la incorporación del Reino Unido al sistema, que se espera tenga lugar a finales de 2014. En todo caso, dicha incorporación no será completa, limitándose a la cooperación policial y judicial en el ámbito penal.

Eurodac

El 29 de junio fue publicado el Reglamento 603/2013 de 26 de junio de 2013, relativo a la creación del sistema Eurodac para la comparación de las impresiones dactilares en aplicación del Reglamento 604/2013, de 26 de junio. Este Reglamento establece los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, así como los aplicables a las solicitudes de comparación con los datos de Eurodac que se presenten por las Autoridades competentes de los Estados miembros y Europol.

Dicho Reglamento, que será de aplicación efectiva el 20 de junio de 2015, presenta como novedad el acceso a la base de datos con los registros de huellas dactilares por parte de las Fuerzas y Cuerpos de Seguridad en relación con la detección, prevención

e investigación de delitos relacionados con el terrorismo y delitos de carácter grave. Esta posibilidad fue severamente criticada tanto por las Autoridades nacionales de Protección de Datos como por el Supervisor Europeo de Protección de Datos, lo que motivó la inclusión en el texto de salvaguardas adicionales cuya efectividad real habrá que evaluar cuando el nuevo sistema entre en funcionamiento.

Oficina de Policía Europea, Europol

La Agencia Española de Protección de Datos ha participado en las actividades de auditoría anual que realiza la Autoridad de Control de Europol. Se ha participado igualmente en las tareas del grupo que se encarga de evaluar los proyectos de Europol que implican la utilización de nuevas tecnologías en el tratamiento de datos de carácter personal y se han mejorado los mecanismos de coordinación con la Unidad Nacional de Europol en España. Asimismo, la Agencia ha colaborado prestando asesoramiento a los departamentos ministeriales involucrados en la negociación del Reglamento.

La Comisión Europea presentó el 27 de marzo una propuesta de Reglamento para sustituir a la Decisión Europol de 2009, de acuerdo a lo establecido en el artículo 88 del Tratado Funcionamiento de la Unión Europea, que incorpora además nuevas funciones y un cambio sustancial en el modelo de supervisión en protección de datos. Esta nueva norma debiera ser aprobada antes de diciembre de 2014, cuando finaliza el periodo transitorio para dichas modificaciones establecido en los protocolos adicionales del Tratado de Lisboa.

La presentación de este proyecto ha provocado controversia en lo referente al modelo de protección de datos incluido en el texto, que para algunos es menos sólido y garantista que el presente en la Decisión de 2009, así como al nuevo modelo de supervisión, que deja atrás el modelo de autoridad de control común y se decanta por una supervisión compartida entre el EDPS y las Autoridades nacionales. En todo caso, el debate sobre el modelo final y la distribución de competencias de supervisión se ha trasladado al Consejo y al Parlamento Europeo, sin que a finales de 2013 se haya producido acuerdo sobre un texto específico.

Sistema de Información de Visados

La Agencia sigue participando de forma regular en las actividades del Grupo de Supervisión Coordinada en protección de datos para el Sistema de Información de Visados, que incluye representantes de las Autoridades nacionales de protección de datos así como del Supervisor Europeo de Protección de Datos.

Definido su programa de trabajo, se ha comenzado a trabajar en diversos aspectos, siendo los más relevantes la gestión de solicitudes de visados, los tratamientos de datos biométricos así como las prácticas de externalización de la gestión de solicitudes de visado, y muy en particular, a la aplicación de la normativa de protección de datos por parte de las entidades contratadas a tal fin por los Estados miembros.

Transferencia de datos de pasajeros, PNR y API

Como se mencionaba al hilo de los comentarios sobre la actividad del GT29, en los últimos años se ha producido un incremento de solicitudes de transferencia de datos de pasajeros desde las aerolíneas a autoridades de cumplimiento de la ley de terceros países con carácter previo a la realización del vuelo.

Los requerimientos de información pueden limitarse a los también citados datos API o extenderse a los datos del registro de nombre de pasajeros (Passenger Name Record o PNR), que contiene toda la información referida a la reserva del viaje que se encuentra en los sistemas de información de la aerolínea o en los del sistema global de gestión de reservas.

Si bien algunas solicitudes se han venido resolviendo a través de acuerdos bilaterales – es el caso de EEUU, Canadá y Australia– otras solicitudes han generado dudas sobre su apoyatura legal, causando problemas a las aerolíneas por la falta de seguridad jurídica y presentando riesgos evidentes en protección de datos ante la falta de información y la ausencia de salvaguardas que mitiguen dichos riesgos.

En lo referido a los acuerdos PNR en vigor, el 1 de julio de 2012 entró en vigor el nuevo acuerdo PNR entre la Unión Europea y los EEUU, el tercero desde que en 2001 comenzara este programa. El año 2013 ha visto la primera revisión conjunta de este acuerdo, que ha incluido la visita de un equipo liderado por la Comisión Europea con expertos en protección de datos de Autoridades de los Estados miembros. El informe final, emitido en noviembre, presenta una valoración global positiva, aunque formula una serie de recomendaciones relacionadas con la necesidad de mejorar los procedimientos de disociación de la información, eliminar el uso del acceso directo a los sistemas de las aerolíneas en busca de datos y mejorar los procedimientos de ejercicio de derechos de los individuos que así lo soliciten.

En ese mismo sentido, se ha llevado a cabo la revisión conjunta que establece el acuerdo con Australia, también con participación de expertos de las Autoridades de Protección de Datos. Aunque se finalizó el trabajo sobre el terreno, el informe final de dicha revisión no se espera hasta 2014. Por último, la revisión del acuerdo con Canadá está pendiente.

A lo largo de 2013 se han venido concretando nuevas peticiones por parte de terceros países de datos API y PNR, siendo el caso más significativo el de la Federación Rusa, con evidente impacto en el tratamiento de datos que realizan las aerolíneas. El Grupo de Trabajo del Artículo 29 ha venido trabajando con la Comisión Europea en la definición

de un marco legal para este tipo de transferencias que ofrezca un nivel adecuado de garantías, pues parece evidente que el modelo de acuerdos bilaterales –vigente para EEUU, Canadá y Australia– no resulta práctico en el marco de un número significativo de terceros países realizando dichos requerimientos de información. Resulta, por tanto, necesario reflexionar como ya se ha explicado respecto a los datos API, sobre una norma de alcance europeo que otorgue una base legal a dichas transferencias con las debidas salvaguardas y un nivel de protección de datos acorde con la normativa europea.

D - CONFERENCIA DE PRIMAVERA DE AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS

Entre los días 15 y 17 de mayo se celebró en Lisboa la Conferencia de Primavera de Autoridades de Protección de Datos. En esta edición las reformas en el marco europeo de protección de datos siguieron siendo el tema central de la Conferencia.

La Conferencia adoptó una Resolución, en la línea de otra aprobada en 2012, apoyando el proceso de reforma pero manifestando su opinión de que algunas cuestiones deben ser mejoradas y, sobre todo, de que el proceso no debe dar lugar a una reducción en el nivel de protección ya alcanzado en Europa.

Asimismo se adoptó una Resolución en la que la Conferencia da la bienvenida a las negociaciones para alcanzar una zona de libre cambio entre Europa y EEUU, manifestando su deseo de que si la protección de datos es abordada en el contexto de las negociaciones se salvaguarden los principios y derechos que definen el modelo europeo de protección de datos y, al mismo tiempo, de que las conversaciones comerciales no condicionen la marcha del proceso de reforma interna en la UE.

Finalmente, la Conferencia aprobó otra Resolución en la que muestra su preocupación por la reducción de los estándares de protección que, a su juicio, supone la propuesta de un nuevo Reglamento de EUROPOL.

E - AVANCES EN LA CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Entre los días 23 y 26 de septiembre de 2013 se celebró en Varsovia (Polonia) la 35ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad bajo el lema Privacidad: Una brújula en un mundo turbulento.

En esta edición, y siguiendo los criterios adoptados en la Conferencia de México y ya aplicados en la de Punta del Este, la Sesión Cerrada tuvo un elevado peso específico en el conjunto de la Conferencia, dedicando un día completo al estudio y los debates sobre la *appificación* de la sociedad. El resultado de estos debates se ha plasmado en la Declaración de Varsovia, que contiene diversas propuestas y recomendaciones para hacer frente al impacto sobre la protección de datos del creciente fenómeno del uso de aplicaciones, en particular en entornos móviles.

La Conferencia adoptó también una serie de resoluciones, entre las que pueden destacarse, en primer lugar, una relativa a Derecho Internacional, en la que se constata una vez más la ausencia de un instrumento internacional vinculante de alcance global en materia de protección de datos y se hace un llamamiento a los gobiernos para abogar por la adopción de un protocolo adicional al artículo 17

del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), que debería consolidar los estándares que han sido desarrollados y apoyados por la Conferencia Internacional. Se adoptó, en segundo término una Resolución sobre Dirección Estratégica de la Conferencia, que prevé la creación de un grupo de trabajo ad hoc para desarrollar una serie de tareas orientadas a mejorar el posicionamiento internacional de la Conferencia y mejorar su eficacia y relevancia para los miembros.

En esta Conferencia fueron reconocidas como nuevos miembros las Autoridades de Protección de Datos de Isla de Mauricio y Kosovo, junto con el Defensor del Pueblo de la Ciudad de Buenos Aires (Argentina). Fueron también acreditados como observadores entidades de Corea del Sur, Canadá, Rusia, Singapur, Ecuador y Bremen (Alemania) que desarrollan funciones que se relacionan con la protección de datos.

La Sesión Cerrada aprobó también la continuación de los trabajos del Grupo de Trabajo de Coordinación Internacional para *enforcement*, en el que participa la AEPD, con vistas a incrementar su cooperación con otras redes y dar soporte a la creación de una plataforma que permita el intercambio seguro de información confidencial en el marco de actuaciones coordinadas o conjuntas en este terreno. El Grupo, siguiendo igualmente las decisiones adoptadas en Ciudad de México, celebrará su próxima reunión anual en Manchester (Reino Unido), en el mes de abril de 2014.

Los representantes de la Agencia participaron como ponentes en dos paneles de la Sesión Abierta de la Conferencia, así como en paneles incluidos en las actividades paralelas organizadas por Public Voice y el Proyecto PHAEDRA.

Durante el evento se presentó una única candidatura para organizar la próxima Conferencia Internacional. La propuesta fue aceptada y será la autoridad de Mauricio la responsable de organizar la Conferencia de 2014. En su condición de autoridad organizadora, Mauricio se integra en el Comité Ejecutivo de la Conferencia, sustituyendo a Uruguay.

F - NUEVOS DESARROLLOS EN LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

Durante el año 2013 se ha consolidado el desarrollo normativo en la Red Iberoamericana de Protección de Datos a través de regulaciones reglamentarias y sectoriales. Proceso al que se añaden nuevas regulaciones sobre protección de datos personales en países que carecían de esta normativa. Perú ha sido el más activo al aprobar, de una parte, el Reglamento de desarrollo de la Ley N.º 29733 general de protección de datos mediante el Decreto Supremo N.º 003-2013-JUS, de 21 de marzo de 2013 y, de otra, entre la normativa sectorial, la Ley N.º 30024, por la que se crea el Registro Nacional de Historias Clínicas Electrónicas, publicada el 22 de mayo de 2013; la Ley N.º 30096 de Delitos informáticos, publicada el 22 de octubre de 2013; y la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, aprobada en octubre de 2013.

Igualmente, hay que destacar la Ley N.º 33, de 25 de abril de 2013, de creación de la Autoridad Nacional de Transparencia y Acceso a la Información de Panamá y, la Ley Orgánica de Protección de Datos de Carácter Personal de la República Dominicana N.º 172-13, de 13 de diciembre de 2013.

En lo que se refiere a la normativa aún en proyecto, deben reseñarse sendas iniciativas legislativas

en Brasil y en Chile (esta última mediante el Proyecto de Ley que introduce modificaciones a la Ley 19.628 sobre Protección de la Vida Privada), que se encuentran aún en proceso de tramitación parlamentaria. Asimismo, conviene reseñar la elaboración de un anteproyecto de ley en esta materia, impulsado desde el Instituto de Acceso a la Información Pública de Honduras.

Por otra parte, del 15 al 17 de octubre se celebró en el Centro de Formación de la AECID, en Cartagena de Indias (Colombia), el XI Encuentro Iberoamericano de Protección de Datos. Al mismo asistieron representantes de las distintas Autoridades de Protección de Datos y altos funcionarios de 19 países iberoamericanos, así como otras entidades públicas iberoamericanas relacionadas con materias de acceso a la información, telecomunicaciones o consumo, entre otras. Igualmente, estuvieron presentes representantes de la Organización de Estados Americanos (OEA), que es miembro Observador de la Red Iberoamericana, y de la Comisión Nacional de Informática y Libertades (CNIL) de Francia; así como una destacada presencia del sector privado, especialmente grandes empresas prestadoras de servicios de internet y telecomunicaciones, y del ámbito financiero y asociaciones empresariales.

El Encuentro abordó cuestiones como el llamado derecho al olvido en el entorno de internet; los servicios en la nube (Cloud computing) y los nuevos modos de publicidad basados en el comportamiento de los usuarios de servicios en internet. En estas cuestiones, las empresas prestadoras de servicios, por un lado, y las Autoridades, por otro, han tratado de poner en común los problemas que estas tecnologías están teniendo en el ámbito de la privacidad, y las posibles soluciones a los mismos para tratar de aunar la defensa de los derechos de los ciudadanos con el desarrollo de la industria.

Asimismo, se debatieron iniciativas tendentes a mejorar la eficacia en el ejercicio de las competencias públicas, impulsando mecanismos de cooperación entre las Autoridades de Protección de Datos con vistas a lograr una aplicación más efectiva de la ley.

Igualmente, se debatió acerca de la Ley Modelo interamericana promovida por la OEA, con la que se pretende establecer un conjunto de principios comunes en esta materia que pueda servir de referencia a las diferentes normativas de los países miembros, y en cuya elaboración la Red Iberoamericana de Protección de Datos (RIPD) está desarrollando un papel muy activo.

De otra parte, en la llamada Sesión Cerrada se aprobó la revisión del Reglamento interno de la RIPD, que supone un nuevo paso en el proceso de institucionalización de esta organización para consolidar una estructura más estable y con un mayor peso de las Autoridades de Protección de Datos, lo que implicará una revisión general del proceso de acreditación de miembros y observadores de la Red. Se aprobó igualmente el Plan anual de Trabajo, cuya iniciativa más destacable es la puesta en marcha de un Grupo de Trabajo de Cooperación, que se encargará de identificar y poner en marcha una actividad de inspección coordinada entre Autoridades de la Red.

El Encuentro concluyó con la aprobación de una Declaración Final en la que se reiteraron y actualizaron los compromisos asumidos por la RIPD.

Por otra parte, la progresiva consolidación normativa e institucional de la protección de datos personales en países latinoamericanos ha multiplicado la convocatoria de foros nacionales e internacionales dirigidos a promover su conocimiento y debatir sobre los nuevos retos que se plantean para garantizar un uso adecuado de la información personal.

De ellos cabe destacar el Seminario Protección de Datos Personales: desafíos jurídicos y tecnológicos, que se celebró en Santiago de Chile coincidiendo con la Cumbre Empresarial de la Comunidad de Estados Latinoamericanos y Caribeños-Unión Europea. La AEPD intervino como ponente en el II Panel Protección de Datos: el modelo español y la situación en Chile.

En el mes de junio tuvo lugar el Primer Congreso Internacional de Protección de Datos - Repensando Paradigmas (Santa Marta, Colombia). La Agencia intervino como ponente en el referido evento, y asistió a la reunión del Comité Ejecutivo de la RIPD, que contó con la presencia de todos sus miembros: México/IFAI (Presidencia), España/AEPD (Secretaría Permanente), Uruguay y Costa Rica, y la Autoridad peruana, como invitada. En dicha reunión se trataron los siguientes asuntos: toma de razón de la admisión de la OEA como nuevo miembro Observador de la RIPD, aprobación del documento sobre Cooperación y aplicación de la Ley, convocatoria y preparación del XI Encuentro y examen del proyecto de Reglamento revisado de la RIPD para su aprobación definitiva en el XI Encuentro.

Asimismo, en el mes de septiembre se celebró en Lima el I Congreso Internacional de Protección de Datos, organizado por la Autoridad Nacional de Protección de Datos Personales de Perú. En la agenda del Congreso, se abordó con detalle la protección de los datos personales en las sociedades actuales, con una ponencia del Director de la Agencia.

En el marco de este proceso de intercambio de información se han intensificado los intercambios de información y experiencias entre Autoridades de la RIPD, tanto en Latinoamérica como en España.

En el mes de febrero se mantuvieron reuniones entre una representación de la AEPD con Comisionados, personal directivo y trabajadores del IFAI en su sede de México D.F. El representante de la Agencia asistió posteriormente al 2.º Foro Nacional de Transparencia y Datos Personales, en Guadalajara, Jalisco, impartiendo una de las dos Conferencias Magistrales relativa al Tratamiento y seguridad del expediente clínico (historia clínica) y su inclusión a las tecnologías de la información: el caso de España.

Asimismo, la AEPD ha colaborado técnicamente con los responsables del Programa Salud.uy, impulsado por la Presidencia de la República Oriental de Uruguay para la implantación de la historia clínica electrónica con la finalidad de equilibrar la asistencia sanitaria en las distintas zonas del país. Su participación se concretó en dos conferencias públicas y cuatro reuniones de trabajo celebradas en Montevideo en el mes de noviembre.

En cuanto a las visitas institucionales, el director de la AEPD recibió las visitas de D. Alejandro Gaitán Durán, Comisionado Presidente de la Comisión Estatal para la Transparencia y el Acceso a la Información Pública del Estado de Durango (septiembre); D. Gerardo Laveaga, Presidente del IFAI y de la RIPD (octubre) y de D. Dante Negro, director del departamento de derecho internacional de la OEA, miembro Observador de la RIPD (noviembre).

Estas actividades se complementaron con el programa de capacitación presencial realizado con la asesora de la Autoridad Nacional de Protección de datos Personales de Perú, en el que se analizaron cuestiones relativas al ejercicio de la función inspectora. La Autoridad Peruana tiene previsto poner en marcha a partir de 2014 las actividades de inspección para hacer plenamente efectivos los mandatos contenidos en la Ley de Protección de Datos y su Reglamento.

<Índice>

5 COLABORACIÓN INSTITUCIONAL CON EL DEFENSOR DEL PUEBLO

Durante el año 2013 se han tramitado un total de 66 asuntos promovidos ante esta Agencia por el Defensor del Pueblo. También debe resaltarse que se atendieron dos solicitudes instadas por el Defensor del Pueblo de Navarra y el Valedor do Pobo de Galicia.

En lo referente a las materias o asuntos afectados, el bloque más destacado —con 22 asuntos— es el relativo a internet, y en especial a la publicación de datos personales en páginas web, blogs, medios digitales y buscadores a efectos de posibilitar su eliminación. Le sigue —con 13 casos— el bloque de temas relacionados con los llamados ficheros de solvencia patrimonial y crédito, por la inclusión en ellos infringiendo alguna de las garantías establecidas en la normativa de protección de datos personales, como falta de requerimiento previo o deuda incierta, entre otros.

A continuación se encuentra un grupo de asuntos con cifras muy similares: los referentes a las comunicaciones comerciales no deseadas, principalmente el llamado spam telefónico (6); los servicios de telecomunicaciones, en especial la contratación fraudulenta de servicios de telefonía (5); la videovigilancia, en las vías públicas y en las comunidades de propietarios (5); y el tratamiento o cesión indebida de datos, fundamentalmente por parte de las entidades financieras (5).

El resto de temas hace referencia a cuestiones de muy variada índole como la regulación de las notificaciones en el Tablón Edictal de Sanciones de Tráfico (TESTRA), la comprobación de la edad de los menores para registrarse en redes sociales, la nueva política de privacidad de Google o la información sobre expedientes provenientes de la extinta Agencia de Protección de Datos de la Comunidad de Madrid (2).

Atendiendo a los motivos que llevan a los ciudadanos a obtener información a través del Defensor del Pueblo hay que mencionar los relacionados con la tramitación de las reclamaciones planteadas ante la Agencia. Un segundo grupo de motivos es el requerimiento de información que demanda la propia institución del Defensor del Pueblo para el ejercicio de sus potestades de investigación, a fin de proceder a un estudio más profundo o para poder establecer criterios sobre la cuestión suscitada. Así ha ocurrido, por ejemplo, en relación con la nueva política de privacidad de Google, o la elaboración de un cuestionario sobre servicios de telecomunicaciones.

Otro grupo relevante de causas, que han justificado la intervención del Defensor del Pueblo en quince ocasiones, ha sido la disconformidad de los afectados con los criterios establecidos por la Agencia Española de Protección de Datos.

Mención específica merecen los dos escritos promovidos por los defensores del pueblo autonómicos, mediante los cuales se da traslado de unos determinados hechos para su conocimiento por parte de esta Agencia. En ambos casos, una vez analizada la información remitida, se acordó la apertura del correspondiente expediente de actuaciones previas de investigación.

En algunos casos, la cuestión planteada ante el Defensor del Pueblo es una verdadera denuncia o reclamación por presunta infracción de la normativa de protección de datos que debería haberse instado, en su caso, ante la Agencia, y así se ha puesto en conocimiento del afectado. También en ocasiones se solicita información al Defensor del Pueblo sobre la falta de respuesta de una denuncia ante la Agencia, constatándose, tras las comprobaciones oportunas, que en muchas ocasiones ha sido ya resuelta y notificada al afectado en fecha anterior a la queja planteada ante el Defensor del Pueblo.

<Índice>

Finalmente, cinco casos de los suscitados han sido promovidos por organizaciones de consumidores, en ámbitos como los ficheros de solvencia (2), las contrataciones fraudulentas en servicios de telefonía (2) o las guías telefónicas en internet (1).

6 COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS

El ejercicio de las funciones atribuidas a las distintas Autoridades de Protección de Datos, —Agencia Española de Protección de Datos, Autoridad Catalana y Agencia Vasca de Protección de Datos—, puso de manifiesto la necesidad de establecer mecanismos de cooperación entre todas ellas para garantizar la igualdad de todos los ciudadanos respecto del derecho fundamental a la protección de datos de carácter personal, estableciéndose un modelo de cooperación mediante reuniones periódicas de sus directores y de grupos de trabajo especializados por razón de las materias a tratar.

Además de las dos reuniones anuales de directores para el intercambio de información y opiniones relacionadas con la actividad de las Agencias, las actuaciones desarrolladas este año en el marco de la cooperación con las agencias autonómicas se han centrado en la coordinación de las actividades de los Registros de ficheros, cuyo objetivo es facilitar el cumplimiento de la obligación de notificación que incumbe a los responsables de los ficheros en Cataluña y en el País Vasco a través de un solo Registro.

De estas actuaciones cabe destacar el seguimiento del protocolo de intercambio de información, cuya finalidad es, por un lado, la actualización y sincronización de las inscripciones de ficheros en los Registros para que el derecho de los ciudadanos a conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y sus responsables, a través de la consulta al Registro General de Protección de Datos, resulte efectivo y, por otro, facilitar el cumplimiento de la obligación de notificación de los responsables de los ficheros.

<Índice>

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA 2013

LA AGENCIA EN CIFRAS

<Índice>

1 INSPECCIÓN DE DATOS

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Escritos de reclamación de tutela	2.230	2.193	1.997	18,83	-8,94
Escritos de denuncia	7.648	8.594	8.607	81,17	0,15
TOTAL	**9.878**	**10.787**	**10.604**	**100**	**-1,70**

DENUNCIAS Y RECLAMACIONES RESUELTAS

TIPO	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Reclamaciones de tutela de derechos	1.939	2.163	2.108	19,63	-2,54
Denuncias	5.917	8.832	8.633	80,37	-2,25
TOTAL	**7.856**	**10.995**	**10.741**	**100**	**-2,31**

<Índice>

RESOLUCIONES - EJERCICIO DE LA POTESTAD SANCIONADORA

SEGÚN TIPO DE PROCEDIMIENTO	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Desistimiento por art. 42 y 71 LRJPAC	337	448	415	5,45	-7,37
Acuerdo de inadmisión a trámite	2.993	4.756	5.114	67,18	7,53
Archivo de actuaciones previas de investigación	901	1.153	1.087	14,28	-5,72
Resolución de procedimientos de apercibimiento	290	316	219	2,88	-30,70
Resolución de procedimientos sancionadores	674	646	719	9,45	11,30
Resolución de procedimientos de infracción de las AAPP	99	38	58	0,76	52,63

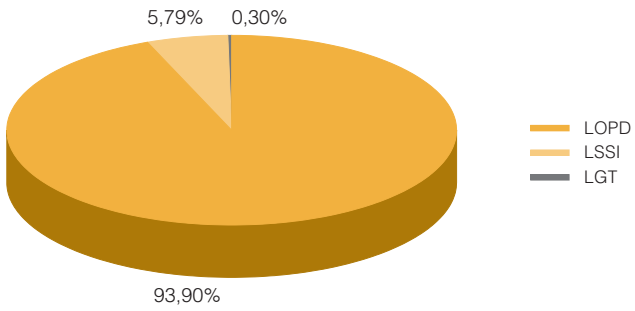
SEGÚN SENTIDO DE LA RESOLUCIÓN	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Archivo actuaciones previas	4.231	6.357	6.616	86,92	4,07
Archivo de procedimiento de apercibimiento	7	10	13	0,17	30
Archivo de procedimiento sancionador	140	89	103	1,35	15,73
Archivo de procedimiento de infracción de las AAPP	18	5	6	0,08	20
TOTAL RESOLUCIONES DE ARCHIVO	4.396	6.461	6.738	88,52	4,29
Declarativa de infracción con apercibimiento	312	306	206	2,71	-32,68
Declarativa de infracción con sanción económica	505	557	616	8,09	10,59
Declarativa de infracción de las AAPP	81	33	52	0,68	57,58
TOTAL RESOLUCIONES DECLARATIVAS DE INFRACCIÓN	898	896	874	11,48	-2,46
TOTAL RESOLUCIONES POTESTAD SANCIONADORA	**5.294**	**7.357**	**7.612**	**100**	**3,47**

* En cada resolución puede haberse analizado más de una infracción.

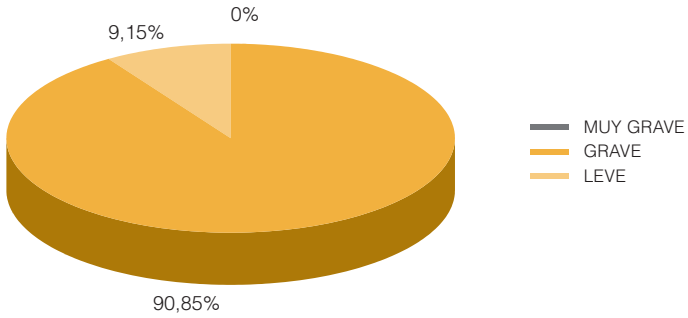
<Índice>

1

INFRACCIONES SEGÚN LEY INFRINGIDA



INFRACCIONES SEGÚN GRAVEDAD



* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

<Índice>

GRADUACIÓN DE LA CUANTÍA DE LA MULTA EN TRATAMIENTOS DE TITULARIDAD PRIVADA (LOPD)

ATENUACIÓN DE LA MULTA / APERCIBIMIENTO	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Apercibimiento por aplicación del art. 45.6	355	352	216	23,38	-38,64
Aplicación del art. 45.5 en sanción económica	145	308	350	37,88	13,64
Aplicación del art. 45.4 en sanción económica	291	201	208	22,51	3,48
Sanción económica sin atenuación	136	166	150	16,23	-9,64
TOTAL INFRACCIONES LOPD	**927**	**1.027**	**924**	**100**	**-10,03**

* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

EVOLUCIÓN DE LAS INFRACCIONES CON SANCIÓN ECONÓMICA (LOPD)

	2011	2012	2013	VAR. % 2012/2013
TOTAL SANCIONES ECONÓMICAS LOPD	**572**	**675**	**708**	**4,89**

* En este apartado se detallan cifras sobre infracciones declaradas, pudiendo haberse declarado más de una infracción en cada resolución de procedimiento sancionador o de apercibimiento.

<Índice>

1

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS INICIADAS

ACTIVIDAD	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Telecomunicaciones	1.378	2.652	2.256	28,71	-14,93
Entidades financieras	841	1.077	1.566	19,93	45,40
Videovigilancia	871	1.271	918	11,68	-27,77
Servicios de Internet (excepto *spam*)	288	404	424	5,40	4,95
Administración pública	206	267	360	4,58	34,83
Suministro y comercialización de energía/agua	122	393	346	4,40	-11,96
Comunicaciones electrónicas comerciales - *spam* (LSSI)	270	353	344	4,38	-2,55
Publicidad y prospección comercial (excepto *spam*)	98	241	270	3,44	12,03
Profesionales, admón. fincas, comunidades de propietarios	226	221	204	2,60	-7,69
Comercio, transporte, hostelería	105	121	162	2,06	33,88
Recursos humanos, asuntos laborales	135	161	160	2,04	-0,62
Sanidad	110	151	139	1,77	-7,95
Asociaciones, federaciones, colegios profesionales, clubes, fundaciones, ONG's	105	101	100	1,27	-0,99
Medios de comunicación	92	62	98	1,25	58,06
Inscripción de ficheros / Información artículo 5	90	101	94	1,20	-6,93
Seguros	67	59	67	0,85	13,56
Asuntos relacionados con procedimientos judiciales	51	46	62	0,79	34,78
Enseñanza	45	45	50	0,64	11,11
Sindicatos	57	48	48	0,61	0
Fuerzas y cuerpos de seguridad	39	29	47	0,60	62,07
Partidos políticos	46	24	40	0,51	66,67
Documentación desechada sin destruir o borrar	36	32	29	0,37	-9,38
Cookies (LSSI)	-	-	16	0,20	-
Comunicaciones comerciales por fax (LGT)	27	8	9	0,11	12,50
Seguridad privada	8	9	8	0,10	-11,11
Derechos ARCO	12	11	4	0,05	-63,64
Otros	64	77	36	0,46	-53,25
TOTAL ACTUACIONES PREVIAS INICIADAS	**5.389**	**7.964**	**7.857**	**100**	**-1,34**

* Las cifras incluyen las actuaciones de inspección incoadas por denuncia o de oficio (EI), los desistimientos que se producen como consecuencia de no haberse subsanado en plazo las denuncias incompletas (AT) y las denuncias no admitidas a trámite (IT).

<Indice>

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS SANCIONADORES RESUELTOS

ACTIVIDAD	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Telecomunicaciones	249	321	377	52,43	17,45
Entidades financieras	79	90	74	10,29	-17,78
Comunicaciones electrónicas comerciales - *spam* (LSSI)	29	49	67	9,32	36,73
Videovigilancia	122	63	57	7,93	-9,52
Suministro y comercialización de energía/agua	20	32	54	7,51	68,75
Servicios de Internet (excepto *spam*)	23	24	29	4,03	20,83
Publicidad y prospección comercial (excepto *spam*)	15	12	24	3,34	100
Seguros	6	7	7	0,97	0
Comercio, transporte, hostelería	8	8	6	0,83	-25
Asociaciones, federaciones, colegios profesionales, clubes	16	3	5	0,70	66,67
Comunicaciones comerciales por fax (LGT)	6	3	4	0,56	33,33
Partidos políticos	1	5	3	0,42	-40
Recursos humanos, asuntos laborales	20	3	2	0,28	-33,33
Profesionales, comunidades de propietarios, admón. fincas	11	1	2	0,28	100
Sanidad	23	2	1	0,14	-50
Inscripción de ficheros / Información artículo 5	20	1	1	0,14	0
Otros	26	22	6	0,83	-72,73
TOTAL RESOLUCIONES (PS)	**674**	**646**	**719**	**100**	**11,30**

* Se incluyen tanto las resoluciones declarativas de infracción como las de archivo del procedimiento.

1

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS DE APERCIBIMIENTO RESUELTOS (SECTOR PRIVADO)

ACTIVIDAD	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Videovigilancia	204	235	131	59,82	-44,26
Servicios de Internet (excepto *spam*)	26	17	19	8,68	11,76
Asociaciones, federaciones, colegios profesionales, clubes	12	12	14	6,39	16,67
Comercio, transporte, hostelería	4	5	13	5,94	160
Profesionales, comunidades de propietarios, admón. fincas	13	14	11	5,02	-21,43
Recursos humanos, asuntos laborales	4	1	7	3,20	600
Publicidad y prospección comercial (excepto *spam*)	2	1	5	2,28	400
Sanidad	0	3	4	1,83	33,33
Sindicatos	1	1	3	1,37	200
Partidos políticos	1	1	2	0,91	100
Inscripción de ficheros / Información artículo 5	13	6	0	0	-100
Administración pública	1	2	0	0	-100
Otros	9	18	10	4,57	-44,44
TOTAL RESOLUCIONES (A)	**290**	**316**	**219**	**100**	**-30,70**

* Se incluyen tanto las resoluciones de apercibimiento como las de archivo del procedimiento.

<Índice>

RESOLUCIONES DECLARATIVAS DE INFRACCIÓN (SECTOR PRIVADO)

ACTIVIDAD	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Telecomunicaciones	220	289	317	38,56	9,69
Videovigilancia	281	276	176	21,41	-36,23
Entidades financieras	58	77	62	7,54	-19,48
Comunicaciones electrónicas comerciales - spam (LSSI)	26	39	59	7,18	51,28
Suministro y comercialización de energía/agua	19	29	48	5,84	65,52
Servicios de Internet (excepto spam)	42	39	44	5,35	12,82
Publicidad y prospección comercial (excepto spam)	16	10	29	3,53	190
Asociaciones, federaciones, colegios profesionales, clubes, ONG's, fundaciones	19	15	19	2,31	26,67
Comercio, transporte, hostelería	10	9	15	1,82	66,67
Profesionales, comunidades de propietarios, admón. fincas	20	15	11	1,34	-26,67
Recursos humanos, asuntos laborales, sindicatos	22	14	10	1,22	-28,57
Seguros	4	9	6	0,73	-33,33
Sanidad	18	5	5	0,61	0
Partidos políticos	2	4	5	0,61	25
Comunicaciones comerciales por fax (LGT)	5	1	3	0,36	200
Inscripción de ficheros / Información artículo 5	25	7	1	0,12	-85,71
Derechos ARCO	2	2	1	0,12	-50
Medios de comunicación	2	2	1	0,12	-50
Enseñanza	4	6	0	0	-100
Administración pública (entidades Derecho privado)	3	2	0	0	-100
Otros	19	11	10	1,22	-9,09
TOTAL RESOLUCIONES DECL. INFRACCIÓN (PS, A)	**817**	**863**	**822**	**100**	**-4,75**

* En cada resolución de procedimiento sancionador o de apercibimiento puede haberse declarado más de una infracción.

<Índice>

1

SANCIONES ECONÓMICAS IMPUESTAS

	2011	2012	2013	VAR. % 2012/2013
TOTAL SANCIONES	19.597.905,97	21.054.656,02	22.339.440	6,10

SECTORES CON MAYOR IMPORTE GLOBAL DE SANCIONES

PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS

TIPO ADMINISTRACIÓN [1]	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Local	30	22	28	48,28	27,27
Autonómica	18	12	20	34,48	66,67
Estatal	8	4	9	15,52	125
Otras Entidades de Derecho Público	43 [2]	0	1	1,72	-
TOTAL RESOLUCIONES	**99**	**38**	**58**	**100**	**52,63**

[1] En un mismo procedimiento de infracción pueden figurar imputados de distintas administraciones territoriales, computándose tales procedimientos en una sola de las administraciones afectadas.
[2] Se incluyen en este apartado los procedimientos en los que se declaró la infracción por parte de 32 Registros de la Propiedad.
* Se incluyen tanto las resoluciones que declaran infracción como las de archivo del procedimiento.

<Índice>

INFRACCIONES DECLARADAS DE LAS ADMINISTRACIONES PÚBLICAS

TIPO ADMINISTRACIÓN	2011	2012	2013	% RELATIVO	VAR. % 2012/2013
Local	14	22	26	45,61	18,18
Autonómica	21	13	21	36,84	61,54
Estatal	6	5	9	15,79	80
Otras Entidades de Derecho Público	40	0	1	1,75	-
TOTAL INFRACCIONES	**81**	**40**	**57**	**100**	**42,50**

* En cada resolución puede haberse declarado más de una infracción.

PROCEDIMIENTOS DE TUTELA DE DERECHOS RESUELTOS

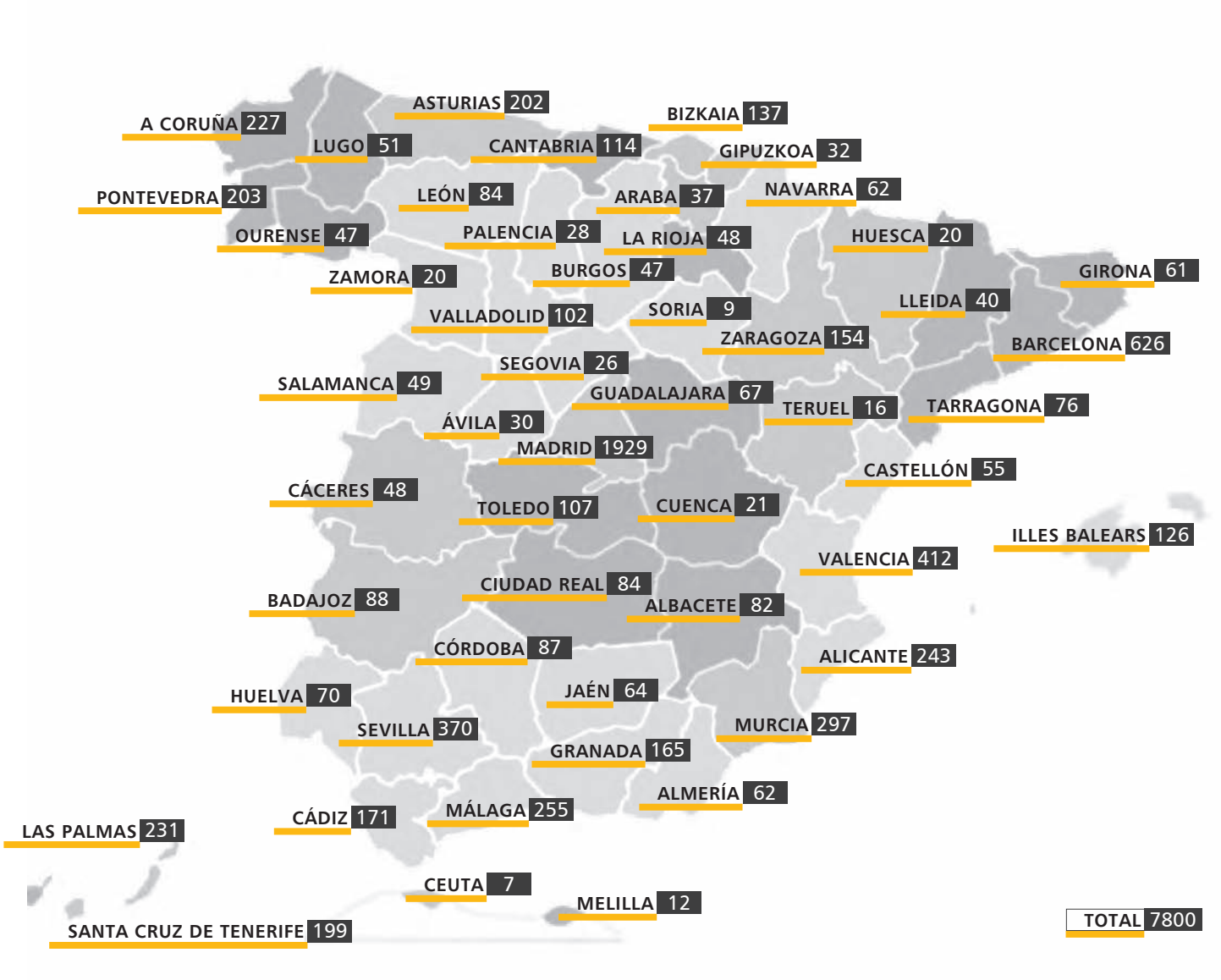
	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMATORIA	ARCHIVO POR INADMISIÓN O DESISTIMIENTO	TOTAL
Cancelación	179	189	143	789	1.300
Acceso	128	138	76	252	594
Rectificación	13	26	10	57	106
Oposición	38	21	26	124	209
TOTAL	**358**	**374**	**255**	**1.222**	**2.209**

* En cada procedimiento resuelto puede haberse tutelado más de un derecho ARCO.

<Índice>

1

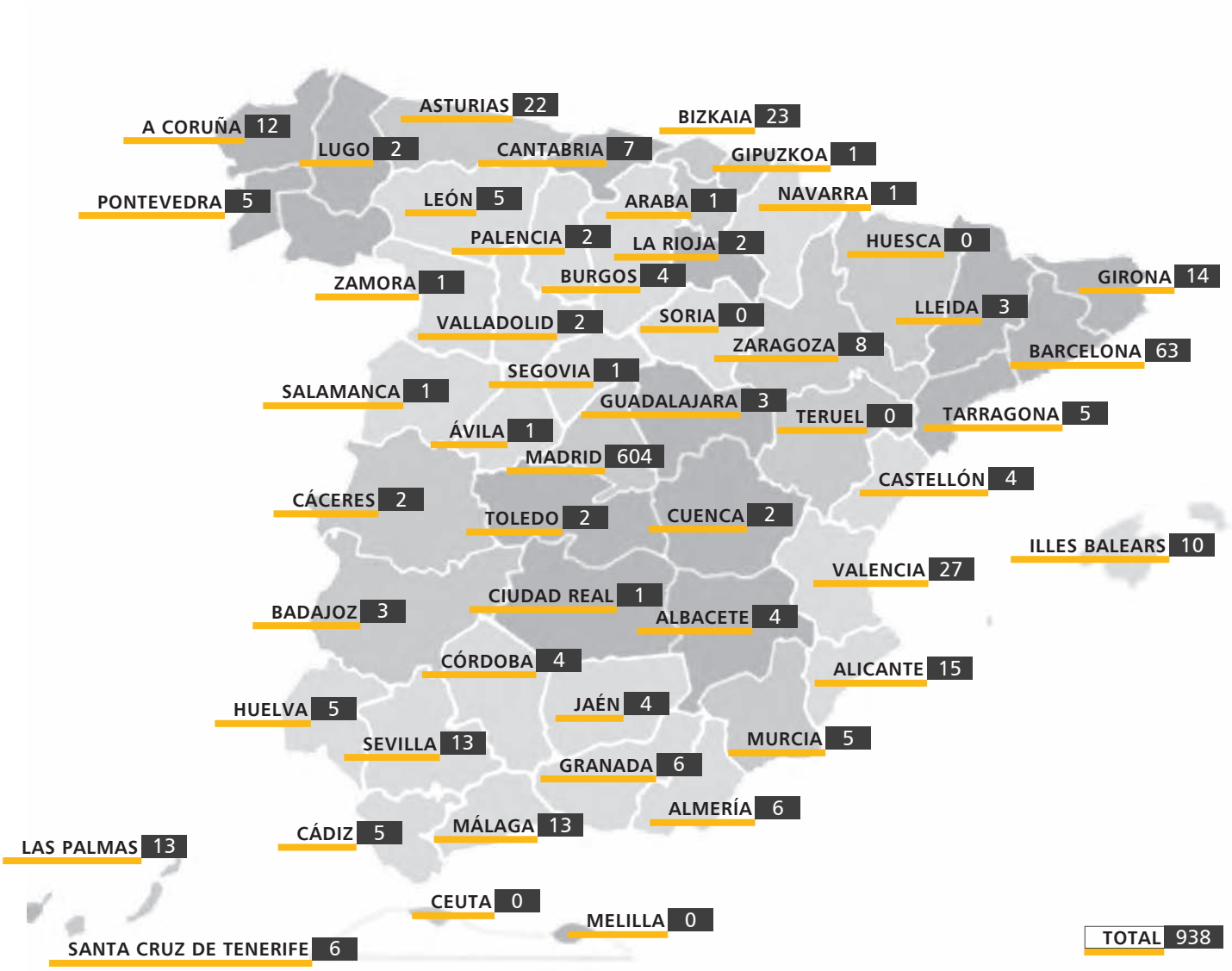
DISTRIBUCIÓN GEOGRÁFICA DE LAS DENUNCIAS PRESENTADAS EN 2013 (PROVINCIA DEL DENUNCIANTE)



* No se consideran las actuaciones previas iniciadas de oficio a iniciativa del Director o las iniciadas por solicitud de colaboración de autoridades extranjeras de protección de datos.

<Índice>

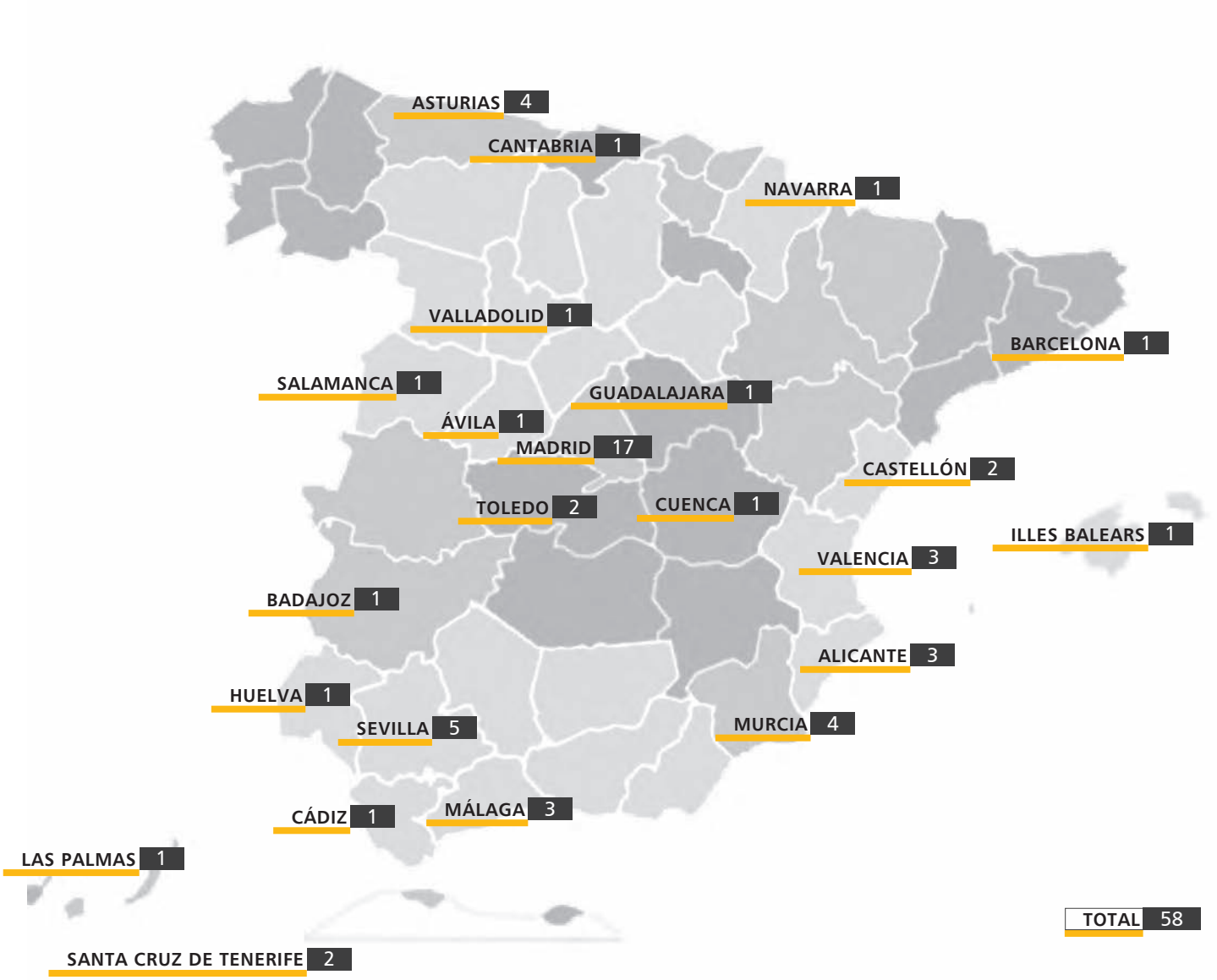
ESTABLECIMIENTO DE IMPUTADOS EN PROCEDIMIENTOS SANCIONADORES Y DE APERCIBIMIENTO RESUELTOS EN 2013



<Índice>

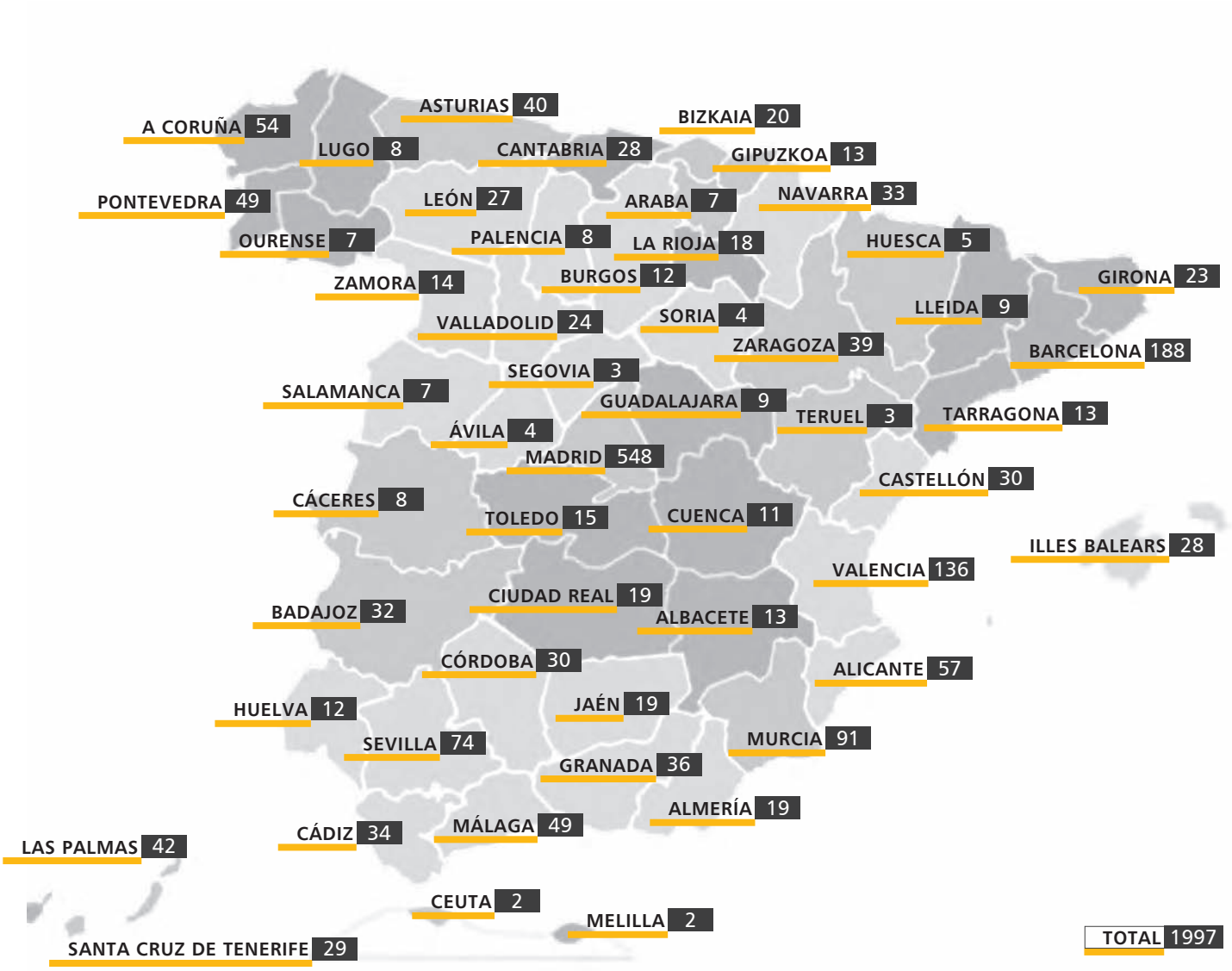
1

SEDE DE LOS IMPUTADOS EN PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS AAPP RESUELTOS EN 2013



<Índice>

DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS EN 2013 (PROVINCIA DEL RECLAMANTE)



<Índice>

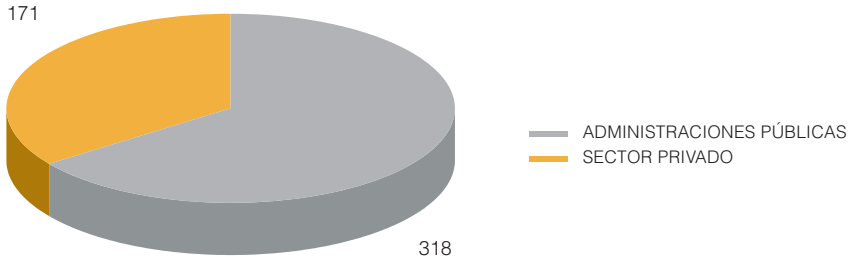
2 GABINETE JURÍDICO

CONSULTAS

ADMINISTRACIONES PÚBLICAS	318
Administración general del Estado	165
Comunidades Autónomas	53
Entidades Locales	59
Otros Organismos Públicos	41

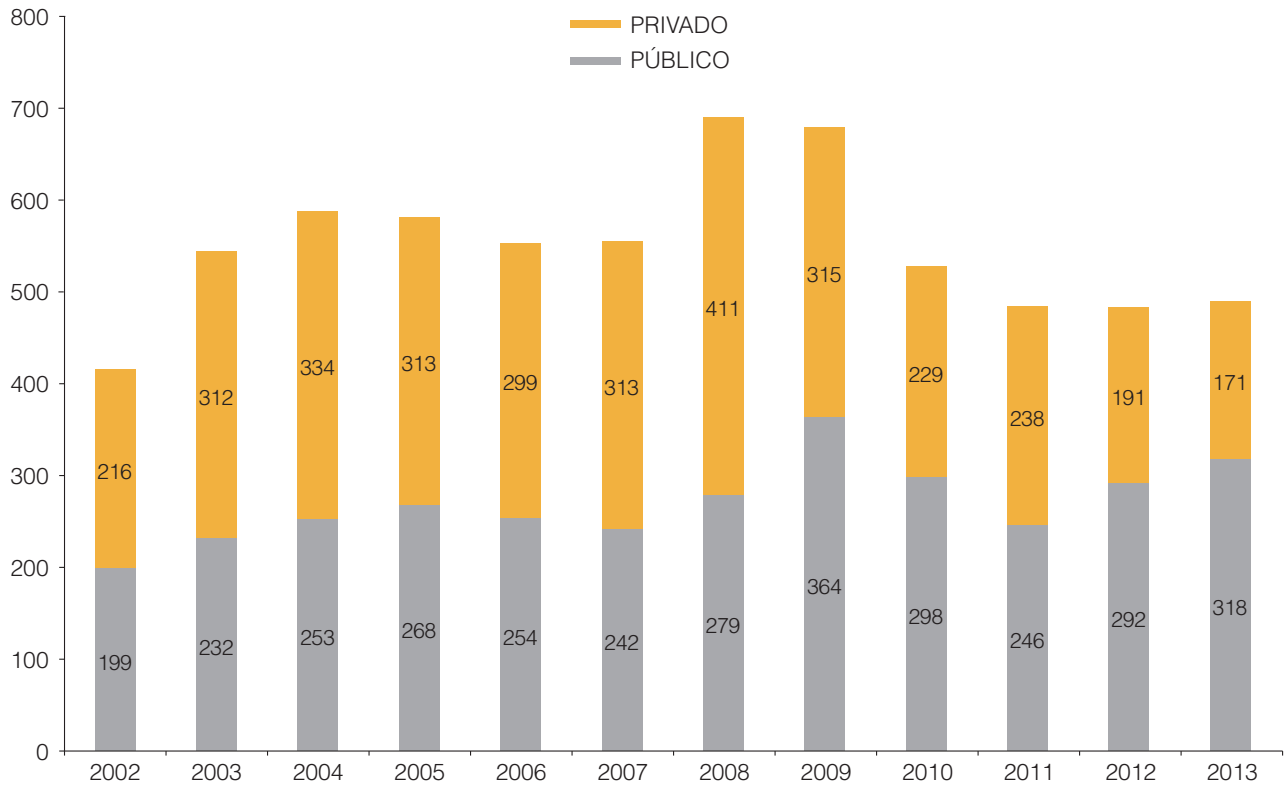
CONSULTAS PRIVADAS	171
Empresas	102
Particulares	27
Asociaciones/Fundaciones	23
Sindicatos/Partidos políticos	18
Otros (Iglesia)	1

DISTRIBUCIÓN 2013 DE CONSULTAS PÚBLICAS/PRIVADAS



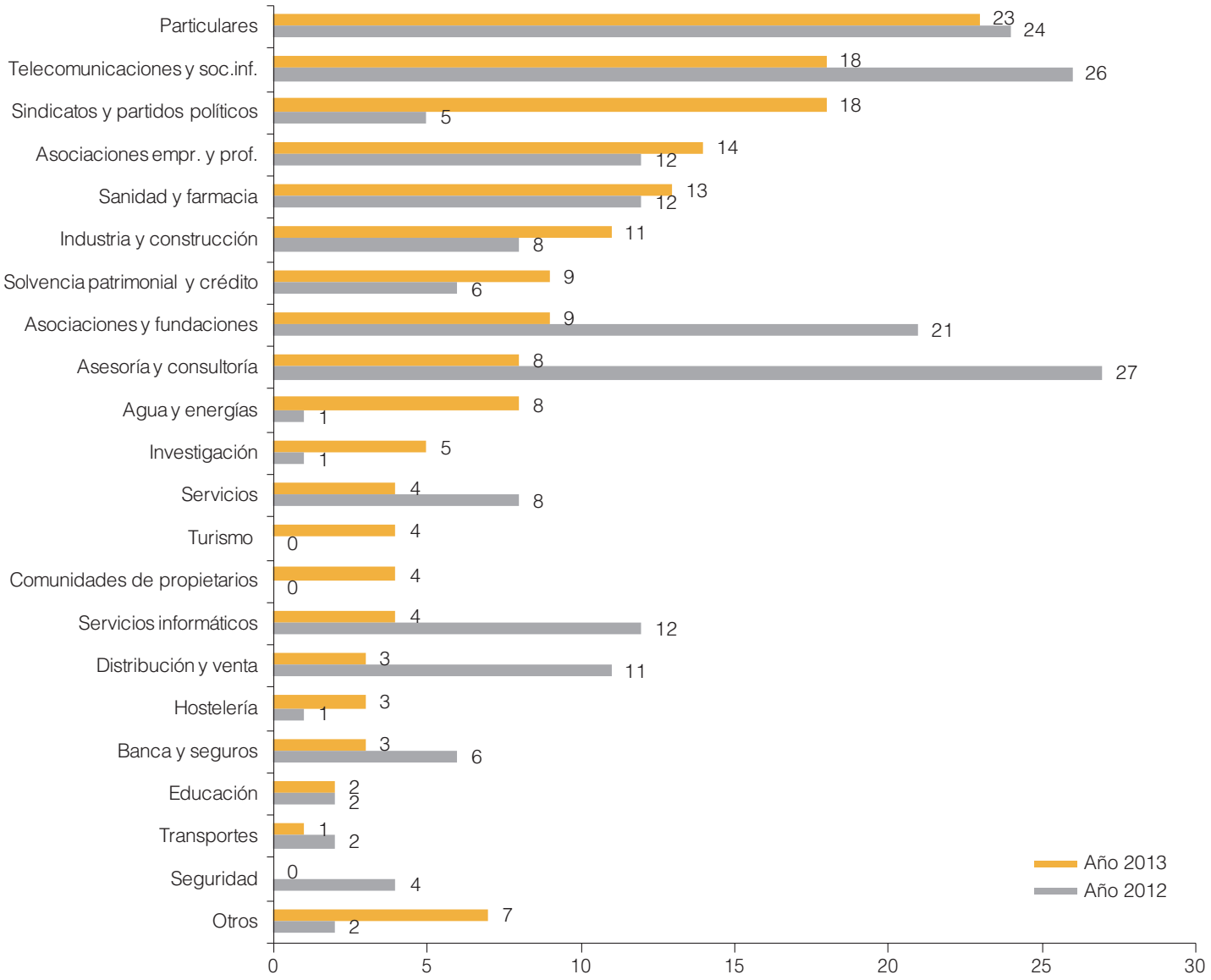
<Índice>

EVOLUCIÓN DE LAS CONSULTAS (2002-2013)



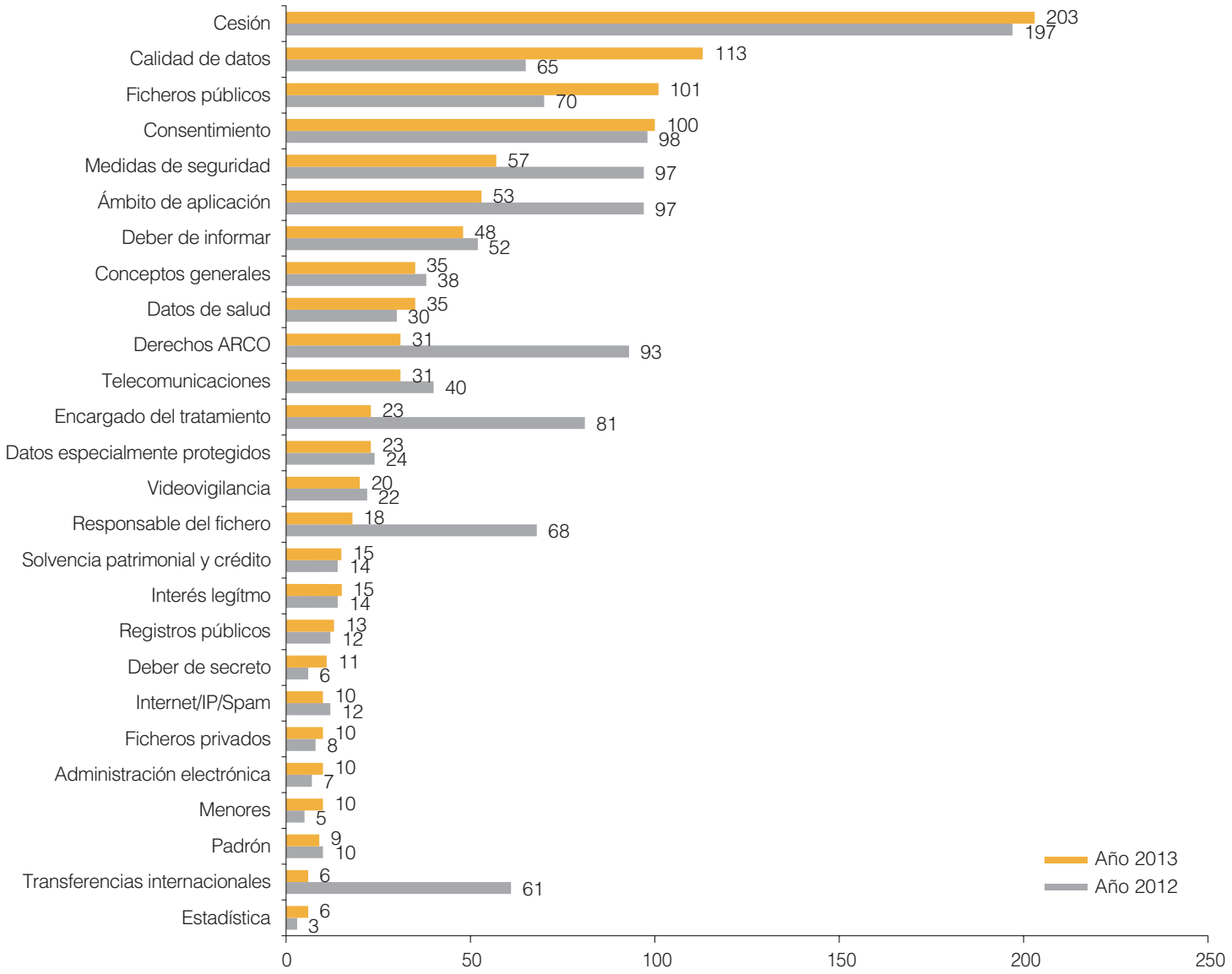
<Índice>

2 EVOLUCIÓN DE LAS CONSULTAS POR SECTORES (2012-2013)



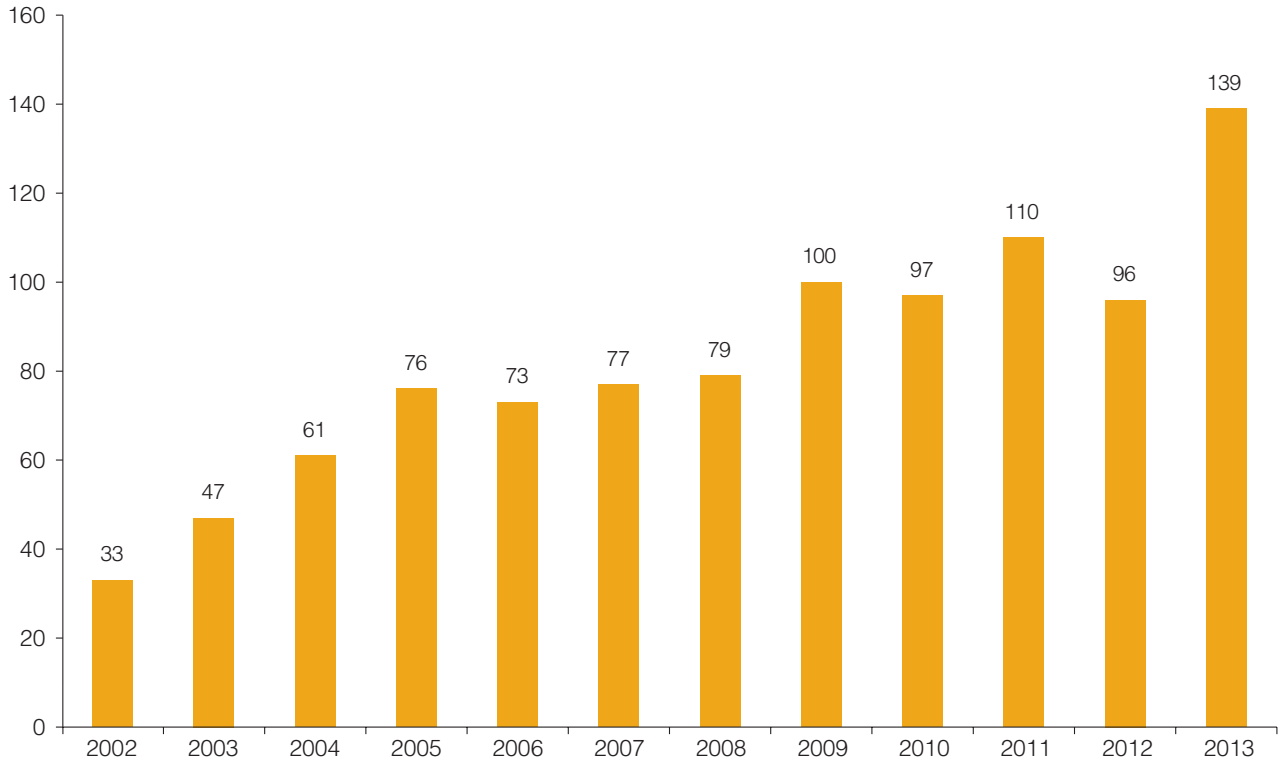
<Índice>

EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS (2012-2013)



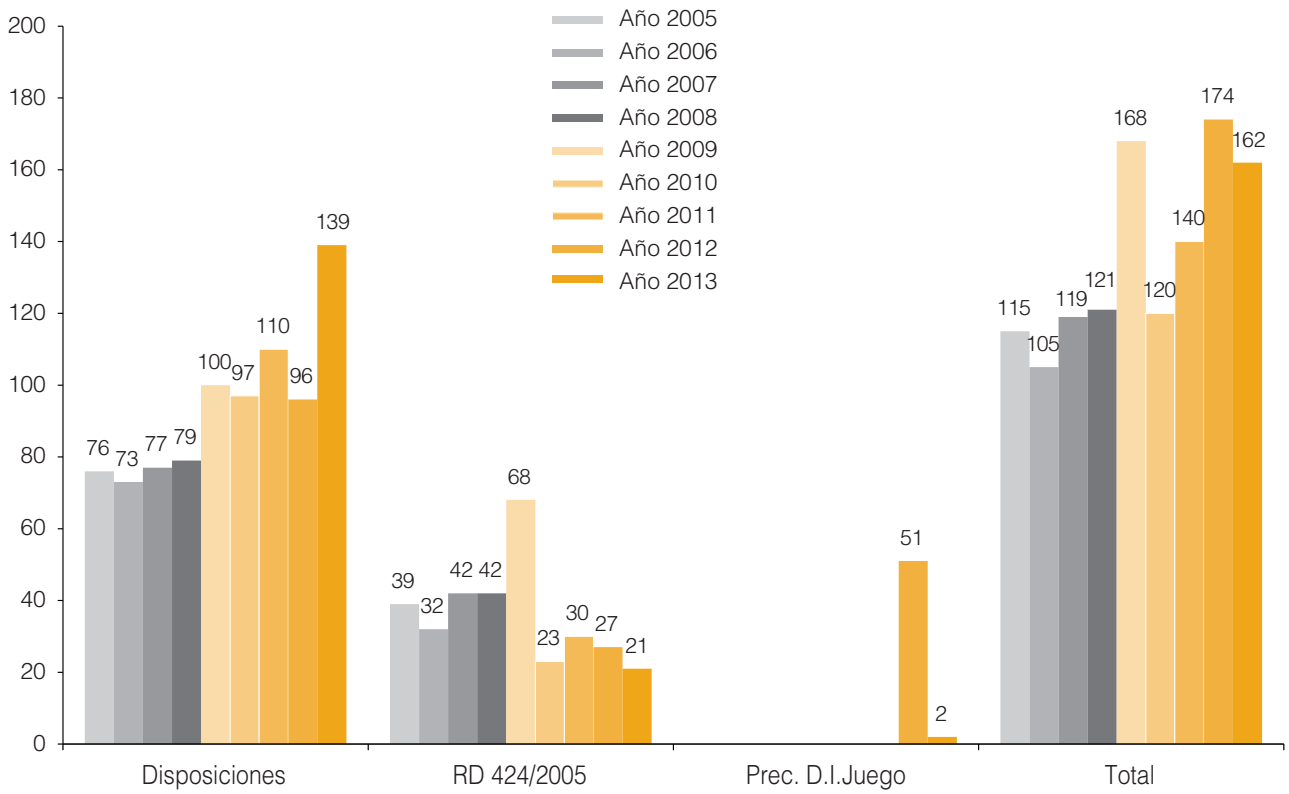
<Índice>

2 EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (2002-2013)



<Índice>

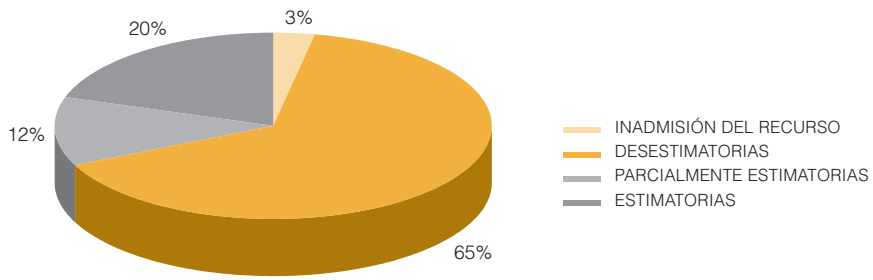
EVOLUCIÓN DE INFORMES PRECEPTIVOS (2005-2013)



<Índice>

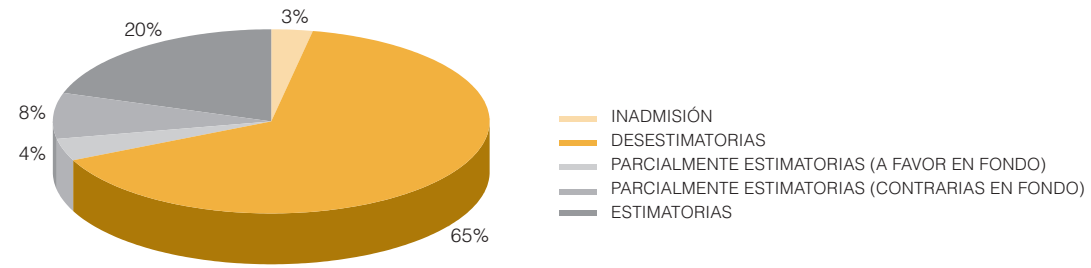
2

SENTENCIAS DE LA AUDIENCIA NACIONAL EN 2013



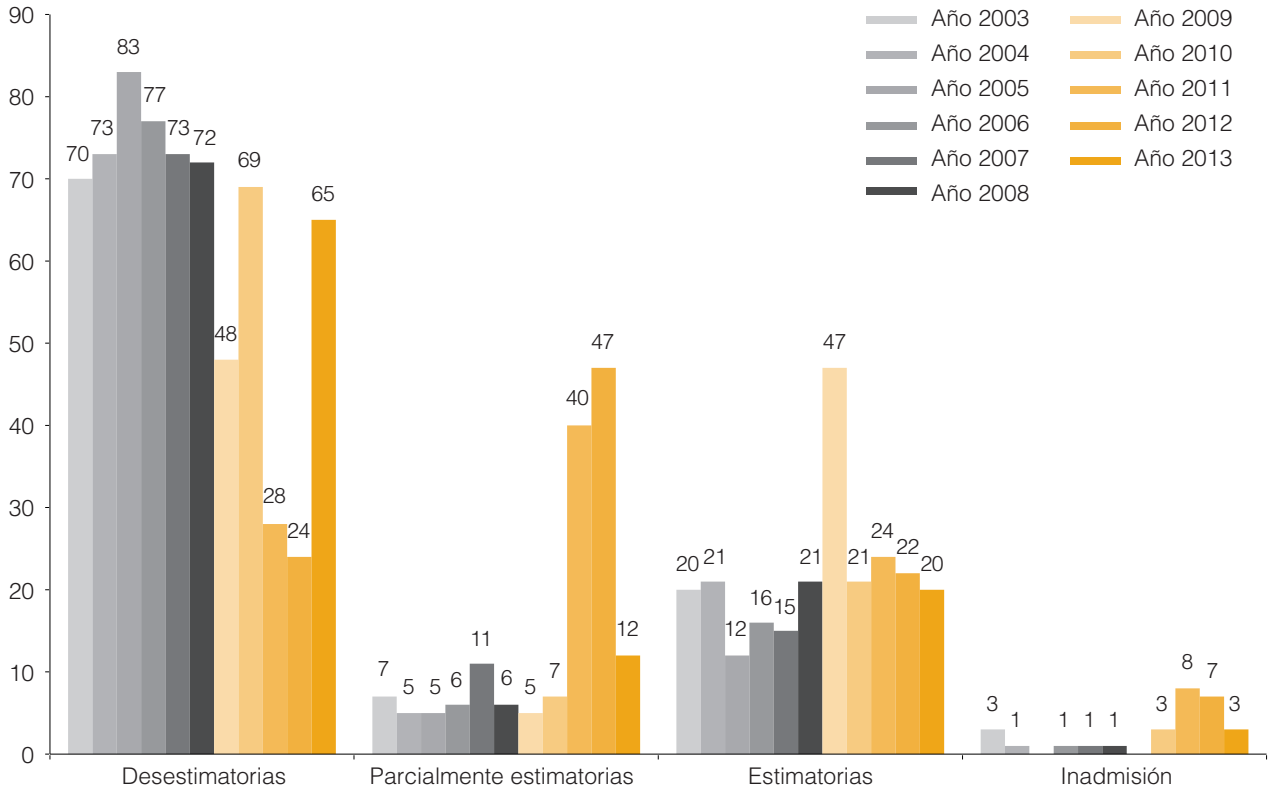
SENTENCIAS PARCIALMENTE ESTIMATORIAS EN 2013

SENTIDO FAVORABLE/CONTRARIO DEL FALLO EN LAS SSAN DE 2013



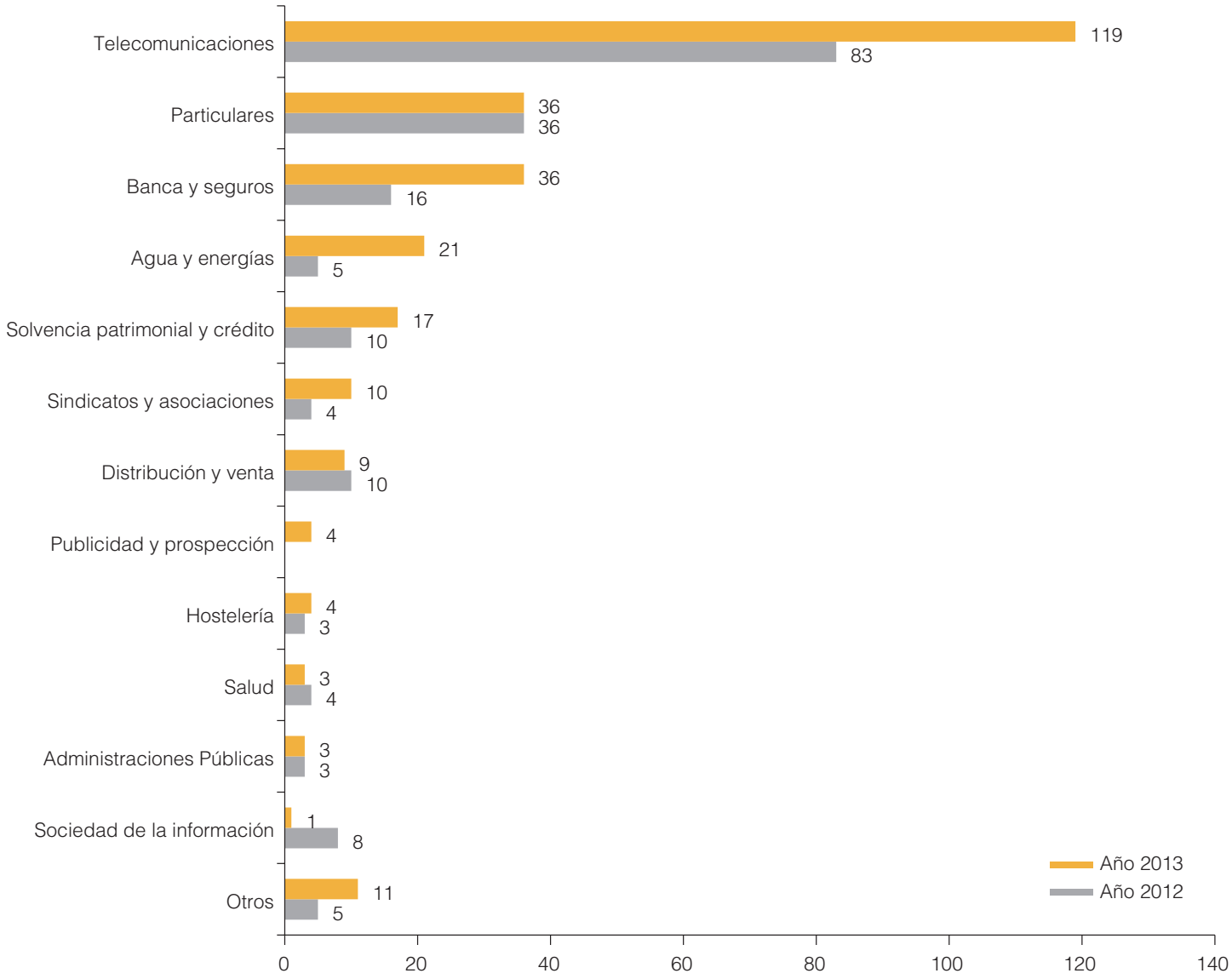
<Índice>

EVOLUCIÓN DEL SENTIDO DEL FALLO EN PORCENTAJES (2003-2013)



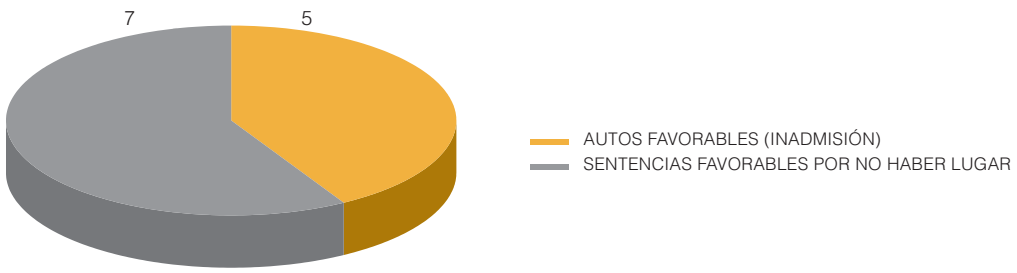
<Índice>

2 COMPARATIVA POR SECTOR DEL RECURRENTE (2012-2013)



<Índice>

SENTENCIAS DEL TRIBUNAL SUPREMO EN 2013



3 ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención telefónica	Atención presencial	Atención por escrito	Total	% de incremento	Consultas de respuesta automática
Año 2011	113.579	3.341	17.715	134.635	28,4%	-
Año 2012	97.162	4.257	10.514	111.933	-16,86%	-
Año 2013	92.942	3.817	5.305 (*)	102.064	-8,81%	105.092

* En el año 2013, **4.637 consultas** fueron presentadas a través de la **Sede Electrónica.**

COMPARATIVA DE ACCESOS A LA PÁGINA WEB

AÑO	2011	2012	2013
Accesos web	2.892.516	4.096.765	4.985.648
Promedio diario	3.961	5.646	6.842

<Índice>

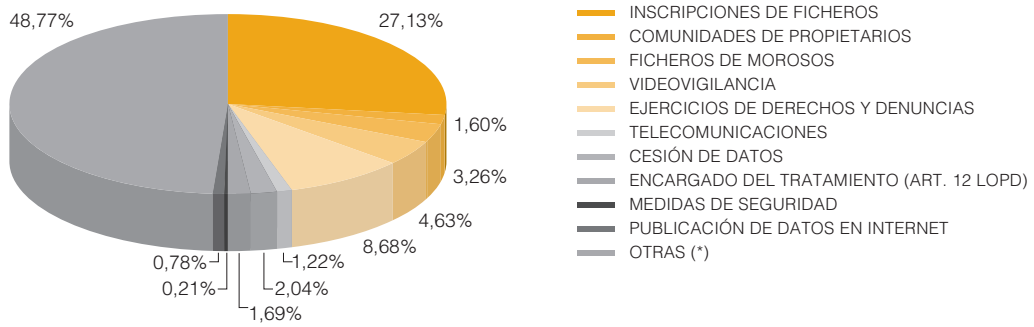
EL USO DE LA SEDE ELECTRÓNICA EN CIFRAS

	2013
Accesos web	4.985.648
Documentos presentados registro electrónico	524
Denuncias	1.942
Reclamaciones de tutela	2.847
Consultas de respuesta automática	105.092
Nuevas consultas de ciudadanos	4.646
Nota. Notificación de ficheros a la Agencia	415.963
Solicitud de copias de contenido de ficheros	14.915
Test Evalúa LOPD	10.589
Test Evalúa Seguridad	3.554
DISPONE	4.828
Consulta y/o descarga de la Guía de seguridad	52.005
Descarga del modelo de documento de seguridad	91.771
Guía del ciudadano	215.299
Guía del responsable	181.255
Guía de videovigilancia	91.469
Guía de relaciones laborales	337.238
Guía de Cloud computing	228.159
Orientaciones para prestadores de servicios de Cloud computing	87.660
Guía de cookies	218.968
Guía RFID	140.354

3 ANÁLISIS DE LAS CONSULTAS POR TEMAS 2013

TEMAS	%
Inscripciones de ficheros	27,13
Comunidades de propietarios	1,60
Ficheros de morosos	3,26
Videovigilancia	4,63
Ejercicios de derechos y denuncias	8,68
Telecomunicaciones	1,22
Cesión de datos	2,04
Encargado del tratamiento (art. 12 LOPD)	1,69
Medidas de seguridad	0,21
Publicación de datos en internet	0,78
Otras (*)	48,77

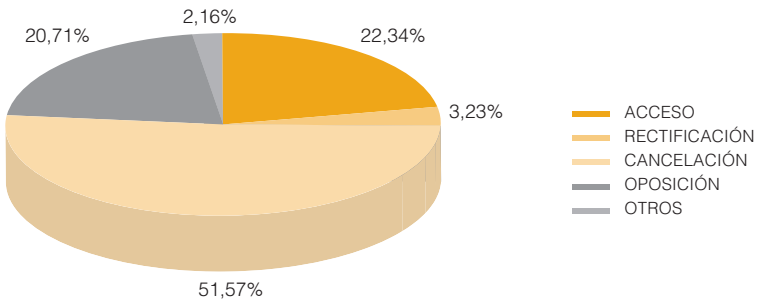
* Este apartado incluye temas como información general sobre la LOPD, direcciones, teléfonos, correos electrónicos, sedes, horarios, búsquedas en la web, transferencias internacionales de datos, competencia de otros organismos públicos, asuntos al margen de la LOPD o delitos en la Red entre otras materias.



<Índice>

ANÁLISIS DE LAS CONSULTAS SOBRE DERECHOS ARCO 2013

DERECHOS	%
Acceso	22,34
Rectificación	3,23
Cancelación	51,57
Oposición	20,71
Otros	2,16

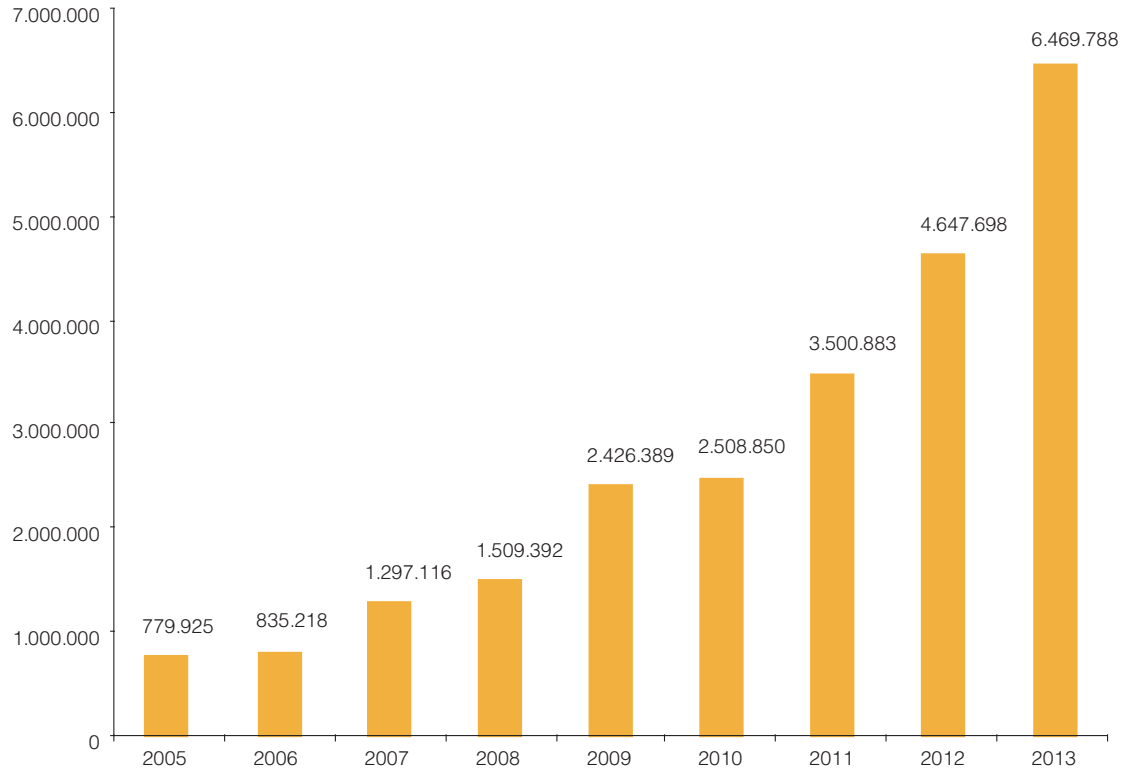


<Índice>

4 REGISTRO GENERAL DE PROTECCIÓN DE DATOS

DERECHO DE CONSULTA AL REGISTRO

Titularidad	2012	2013
Privada	3.380.914	3.409.270
Pública	1.266.784	3.060.518
TOTAL	4.647.698	6.469.788

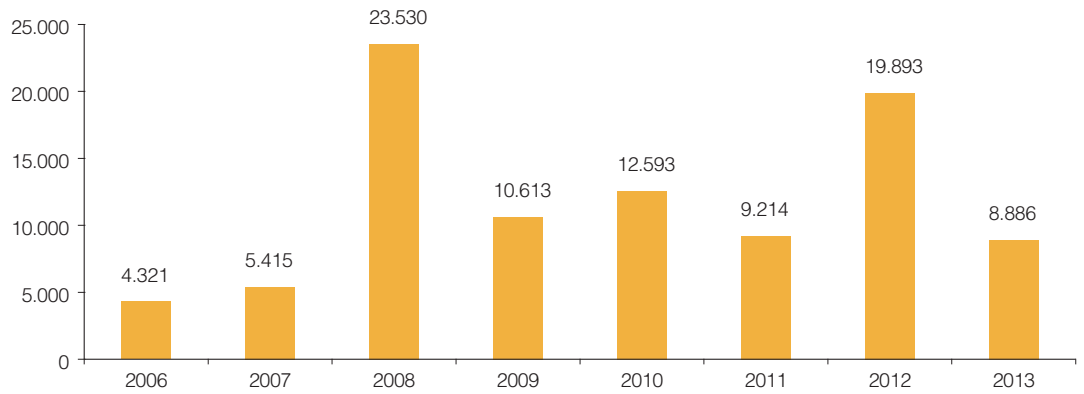


<Índice>

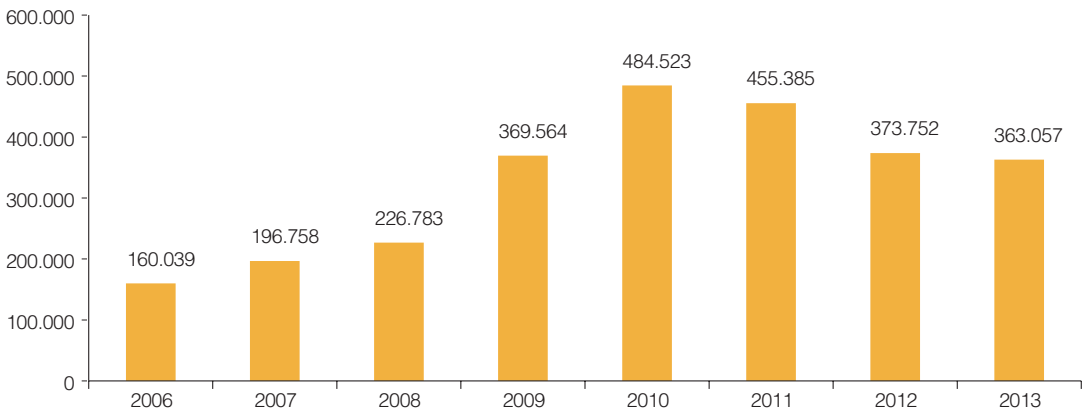
EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

A 31 de diciembre	2006	2007	2008	2009	2010	2011	2012	2013
Titularidad Pública	56.138	61.553	85.083	95.696	108.289	117.503	137.396	146.282
Titularidad Privada	758.955	955.713	1.182.496	1.552.060	2.036.583	2.491.968	2.865.720	3.228.777
TOTAL	**815.093**	**1.017.266**	**1.267.579**	**1.647.756**	**2.144.872**	**2.609.471**	**3.003.116**	**3.375.059**

INCREMENTO ANUAL DE FICHEROS DE TITULARIDAD PÚBLICA



INCREMENTO ANUAL DE FICHEROS DE TITULARIDAD PRIVADA

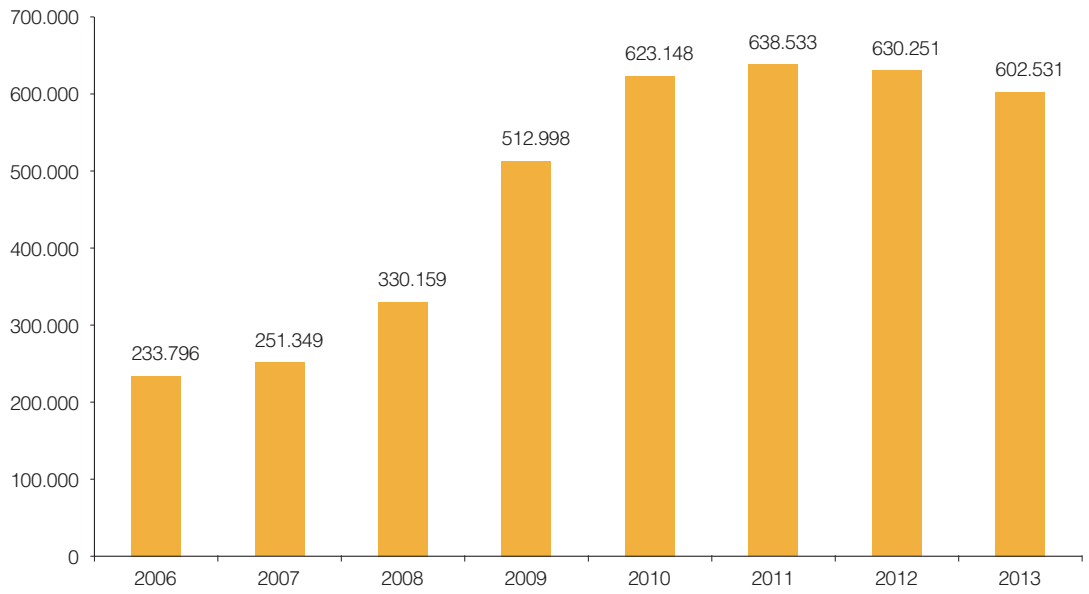


<Índice>

4 OPERACIONES DE INSCRIPCIÓN

	2012	2013	% Variación 2012/13	Media diaria en 2012	Media diaria en 2013
Operaciones de inscripción	630.251	602.531	- 4	2.626	2.511
Total de ficheros inscritos	3.003.116	3.375.059	+12	1.640	1.550

EVOLUCIÓN ANUAL DE LAS OPERACIONES DE INSCRIPCIÓN



<Índice>

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2013	TOTAL	2013	TOTAL
Comunidad Autónoma de Andalucía	**28.843**	**166.601**	**77.149**	**498.759**
Almería	2.865	15.693	8.545	49.473
Cádiz	4.117	20.331	11.350	58.757
Córdoba	2.691	15.707	7.900	47.225
Granada	3.693	22.461	9.233	71.745
Huelva	1.068	7.249	2.733	21.405
Jaén	2.215	12.803	6.269	43.370
Málaga	6.454	38.502	17.533	110.555
Sevilla	5.776	34.591	13.586	96.229
Comunidad Autónoma de Aragón	**5.750**	**39.973**	**12.400**	**98.790**
Huesca	762	7.690	1.672	18.361
Teruel	527	3.528	1.235	9.302
Zaragoza	4.466	28.813	9.493	71.127
Comunidad Autónoma del Principado de Asturias	**7.741**	**35.402**	**17.569**	**106.163**
Comunidad Autónoma de Canarias	**5.969**	**34.609**	**15.890**	**115.562**
Las Palmas	2.852	15.974	8.046	54.944
Santa Cruz de Tenerife	3.121	18.707	7.844	60.618
Comunidad Autónoma de Cantabria	**2.427**	**13.592**	**6.363**	**34.754**
Comunidad Autónoma de Castilla y León	**8.554**	**57.997**	**22.103**	**156.921**
Ávila	633	3.748	1.484	8.887
Burgos	956	9.482	2.305	22.791
León	1.653	11.248	4.037	30.345
Palencia	563	4.313	1.648	11.997
Salamanca	1.045	7.144	2.754	19.323
Segovia	860	4.350	2.261	12.118
Soria	262	2.469	687	6.938
Valladolid	1.935	11.806	5.193	33.013
Zamora	656	3.562	1.734	11.509

<Índice>

4

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2013	TOTAL	2013	TOTAL
Comunidad Autónoma de Castilla-La Mancha	**7.974**	**41.988**	**19.812**	**124.044**
Albacete	1.848	10.841	4.635	34.278
Ciudad Real	2.029	9.497	5.302	28.649
Cuenca	652	4.201	1.665	11.427
Guadalajara	873	4.570	2.160	11.993
Toledo	2.576	12.957	6.050	37.697
Comunidad Autónoma de Cataluña	**27.354**	**217.583**	**70.067**	**564.268**
Barcelona	20.695	161.364	52.004	411.998
Girona	2.971	26.281	7.797	71.104
Lleida	1.289	11.196	3.397	28.449
Tarragona	2.410	19.100	6.869	52.717
Comunidad de Madrid	**37.236**	**193.331**	**85.398**	**488.052**
Comunitat Valenciana	**23.910**	**137.893**	**55.705**	**359.700**
Alicante / Alacant	8.859	47.825	19.981	118.200
Castellón / Castelló	2.385	16.129	5.783	45.363
Valencia / València	12.676	74.093	29.941	196.137
Comunidad Autónoma de Extremadura	**3.613**	**20.029**	**9.142**	**58.323**
Badajoz	2.079	12.640	5.330	36.302
Cáceres	1.536	7.415	3.812	22.021
Comunidad Autónoma de Galicia	**13.145**	**82.031**	**30.909**	**238.552**
A Coruña	6.175	35.923	14.368	103.557
Lugo	1.502	10.447	3.644	28.889
Ourense	1.308	8.871	2.994	24.299
Pontevedra	4.170	26.996	9.903	81.807
Comunidad Autónoma de las Illes Balears	**4.655**	**25.663**	**14.516**	**88.626**
Comunidad Foral de Navarra	**1.932**	**13.015**	**5.271**	**37.735**
Comunidad Autónoma del País Vasco	**7.803**	**47.793**	**20.590**	**128.331**
Araba / Álava	1.262	6.533	2.806	17.209
Gipuzkoa	2.787	15.030	8.200	43.026
Bizkaia	3.761	26.312	9.584	68.096
Comunidad Autónoma de La Rioja	**1.524**	**10.582**	**3.522**	**27.059**
Comunidad Autónoma de la Región de Murcia	**7.085**	**36.121**	**16.666**	**97.090**
Ciudad Autónoma de Ceuta	**232**	**697**	**717**	**1.850**
Ciudad Autónoma de Melilla	**261**	**794**	**1.040**	**3.988**

<Índice>

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPO DE DATOS	2013	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**6.399**	79.430
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**38.864**	380.878
Datos de carácter identificativo	**416.116**	3.228.777
Datos de características personales	**193.205**	1.455.292
Datos de circunstancias sociales	**115.276**	838.647
Datos académicos y profesionales	**112.287**	821.947
Detalles de empleo y carrera administrativa	**122.456**	1.014.159
Datos de información comercial	**119.058**	903.911
Datos económico-financieros	**227.782**	1.850.237
Datos de transacciones	**187.858**	1.370.895
Otro tipo de datos	**20.310**	134.507

4 INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2013	TOTAL	% VARIACIÓN 2013-TOTAL*
Gestión de clientes, contable, fiscal y administrativa	**215.674**	1.938.248	+11,13
Recursos humanos	**93.557**	735.503	+12,72
Gestión de nóminas	**64.694**	549.335	+11,78
Publicidad y prospección comercial	**41.020**	262.279	+15,64
Prevención de riesgos laborales	**39.472**	274.697	+14,37
Videovigilancia	**37.476**	168.290	+22,27
Comercio electrónico	**19.948**	75.824	+26,31
Gestión y control sanitario	**15.569**	132.232	+11,77
Historial clínico	**10.351**	92.227	+11,22
Análisis de perfiles	**7.317**	41.495	+17,63
Seguridad y control de acceso a edificios	**7.279**	47.501	+15,32
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	**5.025**	48.941	+10,27
Educación	**4.708**	40.792	+11,54
Fines estadísticos, históricos o científicos	**3.966**	87.759	+4,52
Servicios económicos-financieros y seguros	**3.782**	66.823	+5,66
Seguridad privada	**3.589**	19.976	+17,97
Prestación de servicios de comunicaciones electrónicas	**3.438**	18.372	+18,71
Cumplimiento/incumplimiento de obligaciones dinerarias	**3.271**	44.608	+7,33
Guías/repertorios de servicios de comunicaciones electrónicas	**3.090**	13.030	+23,71
Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical.	**1.930**	17.855	+10,81
Gestión de asistencia social	**1.706**	13.536	+12,60
Investigación epidemiológica y actividades análogas	**632**	8.630	+7,32
Prestación de servicios de solvencia patrimonial y crédito	**566**	7.966	+7,11
Prestación de servicios de certificación electrónica	**473**	2.860	+16,54
Otras finalidades	**71.158**	506.276	+14,06

* Porcentaje de crecimiento por finalidad declarada.

<Índice>

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2013	TOTAL	% VARIACIÓN 2013-TOTAL
Comercio	**52.275**	380.669	+13,73
Comunidades de propietarios	**43.159**	403.635	+10,69
Sanidad	**32.863**	239.881	+13,70
Turismo y hostelería	**25.864**	153.265	+16,88
Contabilidad, auditoría y asesoría fiscal	**12.930**	145.403	+8,89
Construcción	**11.553**	122.813	+9,41
Educación	**10.705**	79.576	+13,45
Transporte	**8.697**	72.620	+11,98
Asociaciones y clubes	**8.382**	70.657	+11,86
Actividades inmobiliarias	**8.352**	100.335	+8,32
Actividades jurídicas, notarios y registradores	**8.033**	79.343	+10,12
Servicios informáticos	**5.290**	47.531	+11,13
Agricultura, ganadería, explotación forestal, caza, pesca	**4.502**	36.114	+12,47
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	**4.473**	42.180	+10,60
Actividades diversas de servicios personales	**4.166**	32.193	+12,94
Industria química y farmacéutica	**3.874**	55.435	+6,99
Comercio y servicios electrónicos	**3.743**	16.072	+23,29
Maquinaria y medios de transporte	**3.651**	42.851	+8,52
Actividades de servicios sociales	**2.544**	26.906	+9,46
Seguros privados	**2.509**	30.808	+8,14
Actividades políticas, sindicales o religiosas	**2.479**	18.122	+13,68
Sector energético	**2.253**	22.187	+10,15
Producción de bienes de consumo	**2.171**	25.999	+8,35
Activ. de organizaciones empresariales, profesionales y patronales	**2.129**	14.497	+14,69
Servicios de telecomunicaciones	**1.761**	14.559	+12,10
Actividades relacionadas con los juegos de azar y apuestas	**1.622**	8.530	+19,02
Publicidad directa	**1.008**	11.118	+9,07
Entidades bancarias y financieras	**824**	13.092	+6,29
Seguridad	**664**	7.866	+8,44
Inspección técnica de vehículos y otros análisis técnicos	**450**	3.713	+12,12
Organización de ferias, exhibiciones, congresos y otras activ. relac.	**444**	4.016	+11,06
Investigación y desarrollo (I+D)	**397**	4.357	+9,11
Selección de personal	**308**	4.556	+6,76
Actividades postales y de correo	**190**	2.999	+6,34
Solvencia patrimonial y crédito	**81**	1.077	+7,52
Mutualidades colaboradoras de los organismos de la seguridad social	**26**	828	+3,14
Otras actividades	**141.744**	860.290	+16,48

<Índice>

4 INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN	2013	TOTAL
Administración General	777	7.512
Administración CC.AA	752	30.006
Administración Local	10.361	81.973
Otras personas jurídico-públicas	638	26.791
TOTAL	**12.528**	**146.282**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	FICHEROS
Presidencia del Gobierno	8
Ministerio de Asuntos Exteriores y de Cooperación	545
Ministerio de Justicia	148
Ministerio de Defensa	1.745
Ministerio de Hacienda y Administraciones Públicas	607
Ministerio del Interior	224
Ministerio de Fomento	549
Ministerio de Educación, Cultura y Deporte	276
Ministerio de Empleo y Seguridad Social	1.674
Ministerio de Industria, Energía y Turismo	218
Ministerio de Agricultura, Alimentación y Medio Ambiente	411
Ministerio de la Presidencia	57
Ministerio de Economía y Competitividad	490
Ministerio de Sanidad, Servicios Sociales e Igualdad	560
TOTAL	**7.512**

<Índice>

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA - CCAA

	2013	FICHEROS
Comunidad Autónoma de Andalucía	69	1.914
Comunidad Autónoma de Aragón	49	333
Comunidad Autónoma del Principado de Asturias	79	500
Comunidad Autónoma de Canarias	19	442
Comunidad Autónoma de Cantabria	23	230
Comunidad Autónoma de Castilla y León	52	893
Comunidad Autónoma de Castilla-La Mancha	153	814
Comunidad Autónoma de Cataluña	81	9.960
Comunidad de Madrid	68	10.826
Comunitat Valenciana	24	572
Comunidad Autónoma de Extremadura	52	456
Comunidad Autónoma de Galicia	25	315
Comunidad Autónoma de las Illes Balears	10	545
Comunidad Foral de Navarra	8	168
Comunidad Autónoma del País Vasco	1	1.257
Comunidad Autónoma de La Rioja	10	222
Comunidad Autónoma de la Región de Murcia	13	430
Ciudad Autónoma de Ceuta	7	40
Ciudad Autónoma de Melilla	9	89
TOTAL	**752**	**30.006**

<Índice>

4 DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA – ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
Comunidad Autónoma de Andalucía	**843**	**9.887**
Almería	112	1258
Cádiz	49	770
Córdoba	91	849
Granada	192	1.533
Huelva	87	1.211
Jaén	92	808
Málaga	98	1.657
Sevilla	122	1.801
Comunidad Autónoma de Aragón	**559**	**4.876**
Huesca	197	1.654
Teruel	74	464
Zaragoza	288	2.758
Comunidad Autónoma del Principado de Asturias	**83**	**1.333**
Comunidad Autónoma de Canarias	**114**	**1.828**
Las Palmas	50	769
Santa Cruz de Tenerife	64	1.059
Comunidad Autónoma de Cantabria	**66**	**831**
Comunidad Autónoma de Castilla y León	**1.121**	**9.347**
Ávila	91	1.020
Burgos	343	2.557
León	208	1.340
Palencia	119	1.250
Salamanca	92	536
Segovia	27	229
Soria	11	73
Valladolid	188	2.116
Zamora	42	226

<Índice>

	ENTIDADES	FICHEROS
Comunidad Autónoma de Castilla-La Mancha	**458**	**6.822**
Albacete	100	3.472
Ciudad Real	110	848
Cuenca	97	826
Guadalajara	27	370
Toledo	124	1.306
Comunidad Autónoma de Cataluña	**1.044**	**11.987**
Barcelona	443	5.463
Girona	226	2.807
Lleida	213	2.059
Tarragona	163	1.658
Comunidad de Madrid	**230**	**4.606**
Comunitat Valenciana	**499**	**6.897**
Alicante / Alacant	160	2.265
Castellón / Castelló	100	1.029
Valencia / València	240	3.603
Comunidad Autónoma de Extremadura	**307**	**7.614**
Badajoz	186	5.945
Cáceres	121	1.669
Comunidad Autónoma de Galicia	**328**	**4.160**
A Coruña	99	1.418
Lugo	69	766
Ourense	90	994
Pontevedra	70	982
Comunidad Autónoma de las Illes Balears	**85**	**1.541**
Comunidad Foral de Navarra	**238**	**2.457**
Comunidad Autónoma del País Vasco	**339**	**6.316**
Araba / Álava	52	655
Gipuzkoa	126	2.177
Bizkaia	161	3.484
Comunidad Autónoma de La Rioja	**44**	**415**
Comunidad Autónoma de la Región de Murcia	**55**	**1.056**

<Índice>

4

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA OTRAS PERSONAS JURÍDICO PÚBLICAS

	TOTAL
Cámaras Oficiales de Comercio e Industria	469
Notariado	8.069
Universidades	1.456
Colegios Profesionales	2.516
Otros	14.281
TOTAL	**26.791**

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2013	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**436**	19.091
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**1.599**	36.587
Datos relativos a infracciones	**1.141**	24.663
Datos de carácter identificativo	**12.528**	146.282
Datos de características personales	**7.358**	75.592
Datos de circunstancias sociales	**4.215**	38.628
Datos académicos y profesionales	**3.409**	47.268
Detalles de empleo y carrera administrativa	**2.505**	42.829
Datos de información comercial	**2.776**	18.199
Datos económico-financieros	**4.873**	64.132
Datos de transacciones	**2.349**	27.400
Otros tipos de datos	**1.069**	20.963

<Índice>

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES	2013	TOTAL
Datos especialmente protegidos	**436**	19.091
Ideología	**98**	9.289
Creencias	**67**	8.524
Religión	**204**	8.846
Afiliación Sindical	**203**	17.738
Otros datos especialmente protegidos	**1.599**	36.587
Origen Racial	**224**	11.692
Salud	**1.581**	36.412
Vida Sexual	**147**	9.536
Datos relativos a infracciones	**1.141**	24.663
Infracciones Penales	**534**	17.103
Infracciones Administrativas	**1.075**	23.761

<Índice>

4 INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2013	TOTAL	% 2013/TOTAL
Procedimiento administrativo	**2.564**	49.099	+5,22
Recursos humanos	**1.643**	26.202	+6,27
Educación y cultura	**1.418**	16.552	+8,57
Función estadística pública	**1.216**	13.154	+9,24
Gestión contable, fiscal y administrativa	**1.111**	22.508	+4,94
Servicios sociales	**978**	9.775	+10,01
Hacienda pública y gestión de administración tributaria	**791**	10.357	+7,64
Gestión de nómina	**702**	12.493	+5,62
Fines históricos, estadísticos o científicos	**543**	21.152	+2,57
Gestión sancionadora	**524**	5.308	+9,87
Prevención de riesgos laborales	**440**	3.025	+14,55
Publicaciones	**440**	2.099	+20,96
Trabajo y gestión de empleo	**420**	5.856	+7,17
Gestión económica-financiera pública	**403**	6.998	+5,76
Videovigilancia	**395**	2.302	+17,16
Seguridad pública y defensa	**332**	3.960	+8,38
Justicia	**287**	10.613	+2,70
Seguridad y control de acceso a edificios	**273**	3.617	+7,55
Gestión y control sanitario	**272**	4.013	+6,78
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	**243**	2.652	+9,16
Padrón de habitantes	**210**	6.480	+3,24
Prestación de servicios de certificación electrónica	**205**	1.694	+12,10
Historial clínico	**136**	2.423	+5,61
Investigación epidemiológica y actividades análogas	**58**	1.690	+3,43
Otras finalidades	**7.827**	40.176	+19,48

<Índice>

TRANSFERENCIAS INTERNACIONALES DE DATOS

RESOLUCIONES DE AUTORIZACIÓN

		2000-2005	2006	2007	2008	2009	2010	2011	2012	2013	TOTAL AUT.
Estados Unidos 326	EEUU	67	16	10	31	28	25	40	62	47	326
Latinoamérica 421	Panamá	2	-	-	-	-	-	-	-	1	3
	Colombia	1	4	9	4	12	22	23	17	21	113
	Chile	1	7	9	1	8	9	7	1	-	43
	Uruguay	1	1	1	4	3	13	-	2	-	25
	Perú	-	4	5	4	19	20	30	23	23	128
	Guatemala	-	1	-	1	1	-	-	2	1	6
	Paraguay	-	1	1	4	4	1	4	2	-	17
	Brasil	-	-	1	3	-	1	2	2	3	12
	El Salvador	-	-	1	-	-	-	-	-	-	1
	Costa Rica	-	-	1	1	-	1	1	2	1	7
	Nicaragua	-	-	1	-	-	-	-	-	-	1
	México	-	-	-	3	8	20	12	14	7	64
	Ecuador	-	-	-	-	-	1	-	-	-	1
India 179	India	4	3	2	30	28	14	29	27	42	179
Otros países 241	Marruecos	5	2	1	3	8	7	4	10	13	53
	Singapur	1	1	2	-	-	1	2	4	1	12
	Japón	1	-	1	-	1	1	3	4	7	18
	Malasia	1	1	1	-	3	-	-	2	1	9
	Tailandia	1	-	1	-	-	-	-	1	-	3
	Filipinas	-	3	1	5	4	3	5	9	8	38
	China	-	1	1	3	3	1	14	4	6	33
	China (Hong Kong)	-	1	-	-	1	1	-	1	2	6
	Egipto	-	-	1	-	-	-	-	1	1	3
	Nigeria	-	-	1	-	-	-	-	-	-	1
	Túnez	-	-	1	-	-	2	-	3	-	6
	Sudáfrica	-	-	-	3	-	-	-	3	-	6
	Australia	-	-	1	-	7	-	-	3	4	15
	Canadá	-	-	1	-	-	-	-	1	-	2
	Rep. Bielorrusa	-	-	-	3		-	-	-	-	3
	Mónaco	-	-	-	-	1	-	-	-	-	1
	Israel	-	-	-	-	1	6	2	-	-	9
	Vietnam	-	-	-	-	-	3	-	1	-	4
	Barbados	-	-	-	-	-	3	-	-	-	3
	Andorra	-	-	-	-	-	1	-	-	-	1
	Mauricio	-	-	-	-	-	-	1	-	-	1
	Kenia	-	-	-	-	-	-	-	1	-	1
	Serbia	-	-	-	-	-	-	-	1	-	1
	Taiwan	-	-	-	-	-	-	-	2	-	2
	Croacia	-	-	-	-	-	-	-	1	-	1
	Turquía	-	-	-	-	-	-	-	1	-	1
	Ucrania	-	-	-	-	-	-	-	1	-	1
	Bermudas	-	-	-	-	-	1	-	1	-	2
	Nueva Zelanda	-	-	-	-	-	-	-	1	-	1
	Rep. de Corea	-	-	-	-	-	-	-	1	-	1
	Federación Rusa	-	-	-	-	-	-	-	1	1	2
	Emiratos Árabes	-	-	-	-	-	-	-	-	1	1
Internacional 15	Internacional*	-	-	-	-	-	3	1	3	8	15
	Solicitudes presentadas	133	54	127	137	166	197	201	224	192	1.431
	Archivadas	35	17	68	42	24	31	16	52	15	300
	Total Autorizaciones	85	46	43	103	128	155	175	177	170	1.082

* Este apartado incluye las resoluciones que autorizan la transferencia de datos a entidades establecidas en una pluralidad de países.

<Índice>

4

FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES SEGÚN TITULARIDAD

	FICHEROS
Titularidad Privada	13.511
Titularidad Pública	8.328
TOTAL	**21.839**

EVOLUCIÓN DE LAS AUTORIZACIONES DE TRANSFERENCIAS INTERNACIONALES SEGÚN LAS GARANTÍAS APORTADAS (TIPO DE CONTRATO Y NORMAS CORPORATIVAS VINCULANTES -BCR-)

	2006	2008	2010	2011	2012	2013
2001/497/CE[1] Responsable-Responsable	29	50	80	112	167*	195
2002/16/CE[2]- 2010/87/UE[3] Responsable-Encargado	91	216	475	619	735*	861
Encargado-Subencargado[4]					2	9
BCR				1	8	17

[1] DECISIÓN DE LA COMISIÓN, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, modificada por la Decisión 2004/915/CE de 27 de diciembre.

[2] DECISIÓN DE LA COMISIÓN, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (derogada desde 15 de mayo de 2010).

[3] DECISIÓN DE LA COMISIÓN, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[4] Clausulado elaborado por la AEPD para la transferencia internacional de datos de carácter personal entre un prestador de servicios/exportador de datos, establecido en España y un subcontratista/importador de datos, situado en un país que no garantiza un nivel adecuado de protección de datos personales, en el marco de una subcontratación de servicios.

* Los datos de 2012 correspondientes a las transferencias de responsable a responsable y de responsable a encargado han debido ser ajustados para adecuarlos a los criterios de la aplicación de transferencias internacionales.

<Índice>

TRANSFERENCIAS INTERNACIONALES DE DATOS AMPARADAS EN LAS AUTORIZACIONES DE MOVIMIENTOS DE DATOS ENTRE ENCARGADOS Y SUBENCARGADOS DEL TRATAMIENTO

	2012	2013	TOTAL
Ficheros	1	1.561	1.562
Responsables	1	454	455

EVOLUCIÓN DE LA INSCRIPCIÓN DE LOS FICHEROS DE VIDEOVIGILANCIA

AÑO DE INSCRIPCIÓN	TITULARIDAD PRIVADA*	TITULARIDAD PÚBLICA*
1994 - 2006	1.060	17
2007	4.477	85
2008	8.618	161
2009	20.675	264
2010	30.723	777
2011	35.242	485
2012	34.803	561
2013	37.898	471
TOTAL	**173.496**	**2.821**

* Incluye, además de los ficheros que tienen declarada la videovigilancia como finalidad tipificada, aquellos otros en los que se desprende de su denominación o descripción.

<Índice>

4 FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

SECTOR DE ACTIVIDAD PRINCIPAL	2012	2013	% VARIACIÓN 2012-2013
Comercio	32.800	41.599	**+26,83**
Turismo y hostelería	16.433	20.672	**+25,80**
Comunidades de propietarios	10.333	12.831	**+24,17**
Sanidad	7.341	9.230	**+25,73**
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	3.112	3.737	**+20,08**
Construcción	3.074	3.679	**+19,68**
Industria química y farmacéutica	2.680	3.047	**+13,69**
Transporte	2.576	3.000	**+16,46**
Educación	1.874	2.289	**+22,15**
Actividades inmobiliarias	1.807	2.215	**+22,58**
Maquinaria y medios de transporte	1.579	1.930	**+22,23**
Servicios informáticos	1.579	1.889	**+19,63**
Actividades relacionadas con los juegos de azar y apuestas	1.055	1.691	**+60,28**
Contabilidad, auditoría y asesoría fiscal	1.263	1.586	**+25,57**
Sector energético	1.305	1.582	**+21,23**
Seguridad	1.370	1.532	**+11,82**
Asociaciones y clubes	1.222	1.495	**+22,34**
Agricultura, ganadería, explotación forestal, caza, pesca	1.101	1.489	**+35,24**
Producción de bienes de consumo	1.073	1.297	**+20,88**
Servicios de telecomunicaciones	919	1.055	**+14,80**
Actividades diversas de servicios personales	865	1.042	**+20,46**
Actividades de servicios sociales	796	942	**+18,34**
Actividades jurídicas, notarios y registradores	604	804	**+33,11**
Comercio y servicios electrónicos	587	719	**+22,49**
Entidades bancarias y financieras	328	518	**+57,93**
Seguros privados	332	387	**+16,57**
Activ. de organizaciones empresariales, profesionales y patronales	264	345	**+30,68**
Actividades políticas, sindicales o religiosas	247	335	**+35,63**
Inspección técnica de vehículos y otros análisis técnicos	189	232	**+22,75**
Publicidad directa	150	182	**+21,33**
Organización de ferias, exhibiciones, congresos y otras activ. relac.	143	163	**+13,99**
Investigación y desarrollo (I+D)	130	153	**+17,69**
Actividades postales y de correo	85	112	**+31,76**
Selección de personal	35	44	**+25,71**
Mutualidades colaboradoras de los organismos de la Seguridad Social	22	24	**+9,09**
Solvencia patrimonial y crédito	11	15	**+36,36**
Otras actividades	38.339	49.634	**+29,46**
TOTAL	**137.623**	**173.496**	**+26,07**

<Índice>

UNION EUROPEA

SESIONES PLENARIAS GT29 EN BRUSELAS (5):

– 26, 27 febrero 2013

– 15, 16 abril 2013

– 05, 06 junio 2013

– 02, 03 octubre 2013

– 03, 04 diciembre 2013

REUNIONES DE SUBGRUPOS EN LA COMISIÓN EUROPEA (BRUSELAS) A LAS QUE ASISTE LA AEPD (22):

– Subgrupo Futuro de la Privacidad:
- 20 febrero
- 10 abril

– Subgrupo de Tecnología:
- 29, 30 enero
- 25, 26 marzo
- 26, 27 junio
- 02, 03 septiembre
- 05, 06 noviembre

– Subgrupo Borders, Travelers and Law Enforcement (BTLE):
- 07, 08 enero
- 13, 14 marzo
- 10, 11 julio
- 16-18 septiembre
- 20, 21 noviembre

– Subgrupo e-Government:
- 03, 04 abril
- 07, 08 febrero
- 10, 11 julio

– Subgrupo Key Provisions:
- 24 enero
- 18, 19 marzo
- 30 abril
- 25 junio
- 18, 19 septiembre
- 15 noviembre
- 12 diciembre

– Subgrupo World Antidopping Agency WADA:
- 07 febrero

5

OTRAS REUNIONES (18):

– Reunión Grupo DAPIX:
  · 08 enero
  · 29 enero
  · 12 febrero
  · 13 marzo
  · 27 marzo
  · 09 abril
  · 24 abril
  · 29 abril
  · 22, 23 julio
  · 09, 10 septiembre
  · 18 octubre
  · 28, 29 octubre
  · 06, 07 noviembre
  · 10 diciembre

– Datos API:
  · 10, 11 marzo

– DG MOVE Comisión Europea:
  · 23 abril

– Reunión Transfer of Passenger Data to Third Countries:
  · 22 octubre

AUTORIDADES COMUNES DE CONTROL (10)

– Europol-Grupo de Nuevos Proyectos:
  · 27, 28 noviembre

– Europol:
  · 04-08 marzo
  · 29, 30 mayo

– Eurodac:
  · 10-12 abril

– Autoridades de Control de Europol y Aduanas:
  · 04-08 marzo
  · 10, 11 junio
  · 09, 10 octubre
  · 10, 11 diciembre

– Europol, Schengen, Aduanas, JSB:
  · 10, 11 junio

– Grupos de Supervisión Coordinada de los sistemas VIS, SIS y Eurodac:
  · 15-17 octubre

<Índice>

GRUPOS DE TRABAJO SECTORIALES (4):

– Grupo de Telecomunicaciones de Berlín:
  · 14-16 abril (Praga)
  · 2, 3 septiembre (Berlín)

– Grupo de Expertos Retención de Datos en Telecomunicaciones:
  · 9, 10 octubre
  · 17 diciembre

CONFERENCIAS INTERNACIONALES (4):

– Conferencia de Primavera de Autoridades Europeas de Protección de Datos:
  · 15-17 mayo (Lisboa)

– 35ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad
  · 23-26 septiembre (Varsovia)

– 7ª Conferencia de la Asociación Francófona de Autoridades de Protección de Datos:
  · 21, 22 noviembre (Marrakech)

– Encuentro Ibérico:
  · 08-10 noviembre (Oviedo)

OTRAS REUNIONES(5):

– CNIL, París – Google Privacy Policy:
  · 21 enero

– CNIL, París – Google Task Force:
  · 19 marzo

– CNIL, París – Google Task Force:
  · 14 mayo

– Evaluación previa a la incorporación del Reino Unido al Sistema de Información Schengen de Segunda Generación:
  · 22-25 octubre

– Grupo para la mejora de los niveles de seguridad del Sistema de Información Schengen de Segunda Generación (SIS II):
  · 22 de noviembre

<Índice>

6 SECRETARÍA GENERAL

GESTIÓN DE RECURSOS HUMANOS

		DOTACIÓN 31/12/2013	CUBIERTOS 31/12/2013
PUESTOS DE TRABAJO	Funcionarios	157	153
	Laborales	4	2
	Laborales fuera de Convenio	3	2
	Alto cargo	1	1
		165	**158**

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
EFECTIVOS 2013	6	3	21	47	3	15	3	12	2	7	12	22

	A1	A2	C1	C2
EFECTIVOS 2013	31	50	18	58

MUJERES	**89**
HOMBRES	**69**

<Índice>

EVOLUCIÓN DEL PRESUPUESTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

	CRÉDITO EJERCICIO 2011 (EUROS)	CRÉDITO EJERCICIO 2012 (EUROS)	CRÉDITO EJERCICIO 2013 (EUROS)
CAPÍTULO I	6.283.509	6.346.260	6.672.660
CAPÍTULO II	5.805.060	5.474.130	5.024.000
CAPÍTULO III	697.841	546.740	432.450
CAPÍTULO VI	1.625.160	1.539.620	1.372.160
CAPÍTULO VIII	26.400	22.800	22.800
TOTAL	**14.437.970**	**13.929.550**	**13.524.070**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2013

www.agpd.es