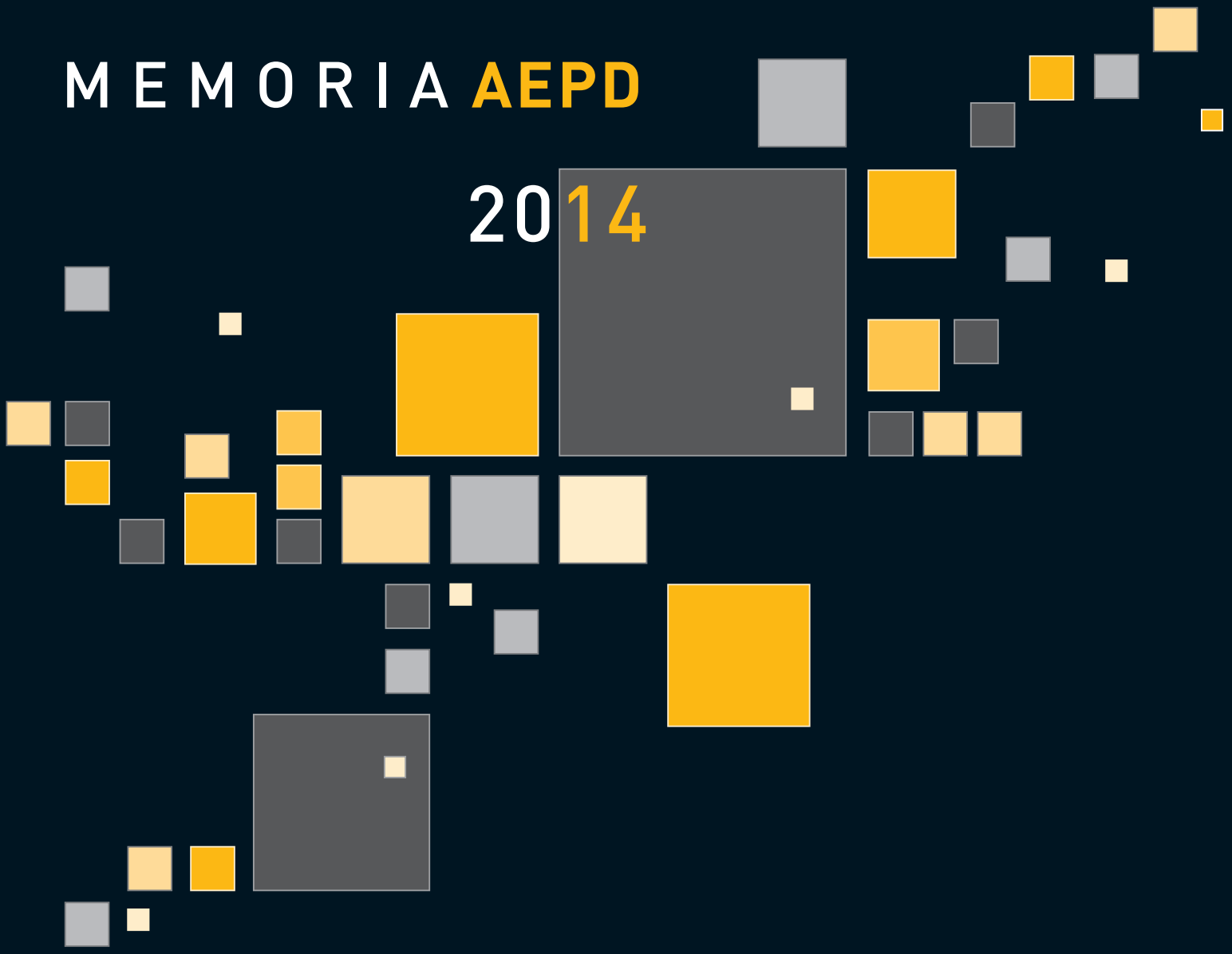
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD

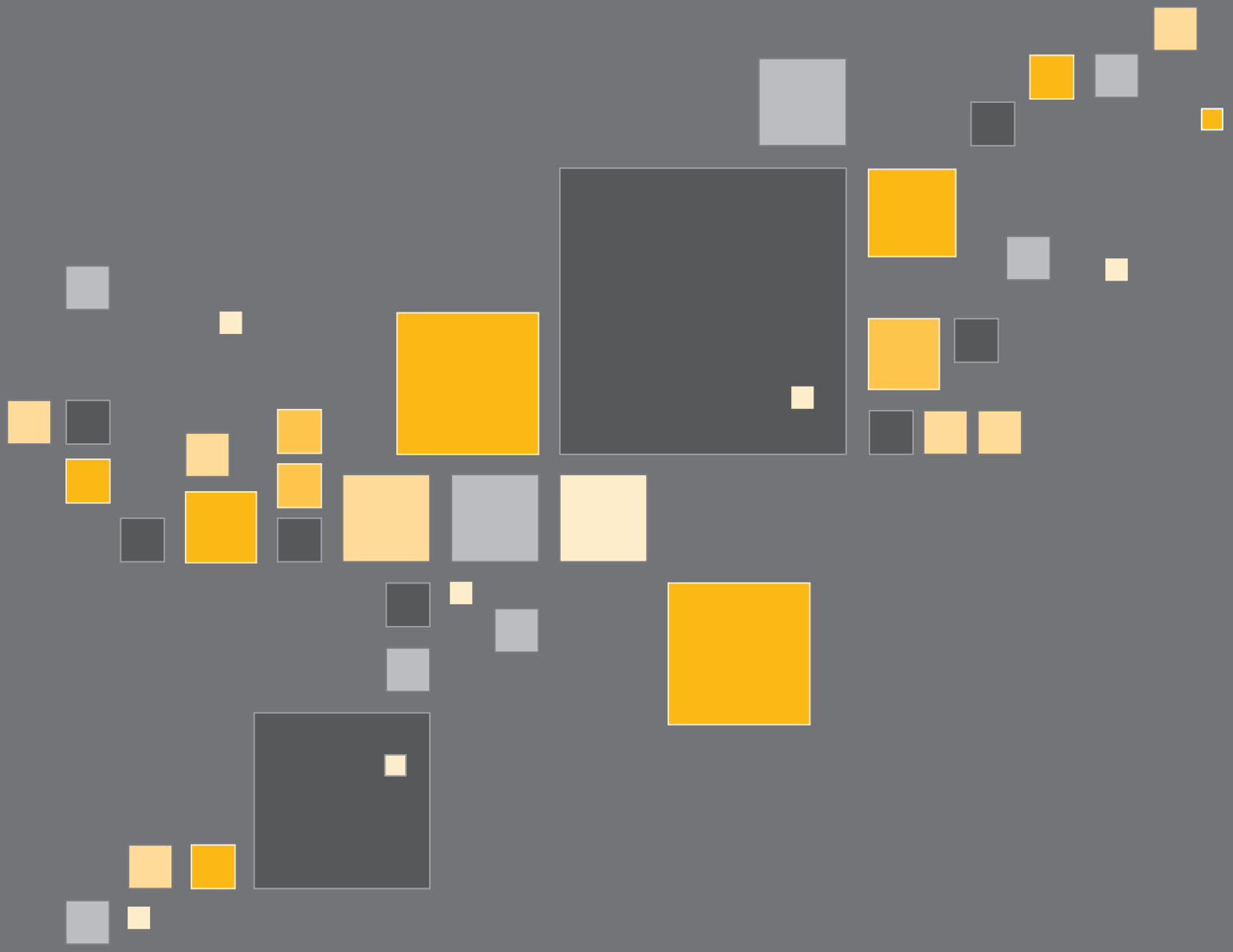
2014



ISSN: 2254-691X
Depósito Legal: M-19499-2015

Imprime: Imprenta Nacional
Agencia Estatal Boletín Oficial del Estado

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



MEMORIA AEPD 2014

PRÓLOGO

Un año más me complace presentarles la Memoria de la Agencia Española de Protección de Datos, que recoge un informe detallado de las actividades realizadas durante 2014, una exposición de las novedades legislativas y jurisprudenciales más relevantes, y un análisis de los principales retos que afronta el derecho fundamental a la protección de los datos personales. Compilar, redactar y presentar en un único texto todos estos materiales supone un gran esfuerzo para todos los implicados en su elaboración que, año tras año, se aborda no sólo con el objetivo de dar cumplimiento a una obligación legal sino también con la vocación de presentar la actuación de la Agencia con un enfoque didáctico, que contribuya a fomentar el conocimiento del derecho y a fortalecer la concienciación ciudadana sobre la importancia de proteger los datos personales en un entorno en el que continuamente surgen nuevos desafíos.

El conocimiento del derecho y la conciencia ciudadana sobre la importancia que su protección tiene para el libre desarrollo de las personas son factores esenciales para afianzar una cultura de la protección de los datos personales que, más allá de la mera garantía formal, posibilite una verdadera salvaguardia efectiva de la intimidad y de la vida privada en las complejas sociedades contemporáneas. De ahí que al inicio de mi mandato estableciera como líneas estratégicas principales fomentar entre los ciudadanos el conocimiento y ejercicio de sus derechos, por un lado, y facilitar a los sujetos obligados la observancia de las normas vigentes, por otro. Y, consecuentemente, hemos considerado necesario, sin renunciar a seguir cumpliendo con las funciones tradicionales, orientar parte de las actuaciones de la Agencia a impulsar el desarrollo de una cultura proactiva de la protección de datos, favoreciendo las actuaciones preventivas y el compromiso responsable de quienes tratan datos personales.

Me complace constatar que ambas líneas han tenido gran aceptación y en las dos hemos conseguido un notable avance, como se refleja en esta misma Memoria y en las de los ejercicios precedentes. La mayoría de los proyectos, herramientas, guías y utilidades diseñadas con estos fines están disponibles en nuestra página web (www.agpd.es), que desde 2012 integra también la Sede electrónica de la Agencia y en la que los interesados pueden realizar todo tipo de trámites sin necesidad de desplazamientos y sin coste alguno. Este año se ha procedido además a la completa revisión y actualización de la web para reforzar su función de canal de comunicación dinámico y permanente, tanto con los ciudadanos como con los responsables de los tratamientos. La nueva página es más ágil e intuitiva, se adapta a la navegación desde los dispositivos móviles e incorpora nuevos contenidos, incluida una sección dedicada a la transparencia institucional en la que se hace pública la información legalmente requerida, complementada con otros datos y documentos que permiten conocer con detalle el funcionamiento y los gastos de la Agencia.

Entre los proyectos desarrollados durante 2014, merece destacarse especialmente la *Guía para una Evaluación de Impacto en la Protección de Datos Personales*, con la que hemos querido contribuir a promover la cultura de la responsabilidad proactiva y de la *privacidad desde el diseño*, proporcionando un marco de referencia flexible para la realización de este tipo de evaluaciones, que han alcanzado ya un gran desarrollo en otros países y que constituyen una herramienta sumamente útil para eliminar o reducir posibles riesgos. A pesar de que actualmente no sean obligatorias, recomendamos vivamente su realización por los indudables beneficios que reportarán a las organizaciones y, aunque no podrán constituir una causa de exención de responsabilidades, si se realizan correctamente la Agencia las tendrá en cuenta como un elemento relevante a la hora de valorar si se ha adoptado la diligencia debida en la implementación de las medidas adecuadas para cumplir con las exigencias legales.

Este enfoque proactivo de la protección de datos y de la privacidad, deseable en todos los sectores, ha de ser uno de los pilares esenciales sobre los que se asiente la evolución de las nuevas tecnologías. Actualmente estamos viendo cómo el volumen de información generada crece exponencialmente al tiempo que se multiplican las capacidades técnicas para tratarla y se incrementa su valor económico, una evolución que va a experimentar un fuerte impulso con la expansión de tecnologías como el Internet de las Cosas o los procesos de tratamientos masivos de datos conocidos como Big Data. Esta continua irrupción de nuevas tecnologías y nuevos procesos de tratamientos de datos en un entorno fuertemente interconectado acrecienta los riesgos de que los individuos pierdan el control sobre su información, por lo que resulta imprescindible reforzar los derechos y las garantías para mantener una protección efectiva de la esfera personal.

A atender esa necesidad se dirige la reforma en curso del marco normativo europeo que, lamentablemente, se está retrasando mucho más de lo deseable. Urge aprobarlo pero sin renunciar a la calidad de los contenidos porque no se debe olvidar que el verdadero objetivo del proceso de reforma es proporcionar a los europeos una protección de sus datos personales reforzada y adaptada a los retos actuales. En este sentido, es trascendental asegurarse el acierto en la elección de los instrumentos idóneos porque el texto finalmente adoptado regirá la práctica de la protección de datos en Europa en los próximos diez o quince años.

Entretanto, la sentencia del TJUE de 13 de mayo de 2014 ha contribuido decisivamente a mejorar la protección de datos en internet. Aunque generalmente se presenta como el reconocimiento de un nuevo derecho, el llamado «derecho al olvido», en realidad el Tribunal no reconoce ningún derecho nuevo sino que únicamente confirma la posibilidad de ejercer los derechos de cancelación y oposición ante las compañías gestoras de los motores de búsqueda, tal y como veníamos defendiendo desde la Agencia. En términos generales, la sentencia se está aplicando con normalidad, tanto en España como en el resto de los países europeos, y varios miles de personas se han beneficiado ya del derecho a proteger su vida privada frente a la divulgación injustificada de informaciones personales. Finalmente, la aplicación de la sentencia ha evidenciado el escaso fundamento de algunas críticas recibidas, particularmente de aquellas que vaticinaban un fuerte impacto en las libertades de expresión y de información.

En el momento en el que escribo estas líneas están a punto de cumplirse cuatro años desde que fui nombrado director de la Agencia, cuatro intensos años en los que hemos tenido que hacer frente a retos muy complejos en un difícil contexto de crisis económica, restricciones presupuestarias y congelación de plantilla. Que los desafíos se hayan podido superar con éxito ha sido posible gracias al magnífico equipo de funcionarios y empleados públicos que trabajan en la Agencia a los que, una vez más, tengo que agradecer su esfuerzo para hacer frente a una carga de trabajo que ha ido en constante crecimiento, tanto cuantitativo como cualitativo, a lo largo de estos años. Su compromiso, profesionalidad y buen hacer serán siempre recordados con gratitud por quien ha tenido el honor de ser su director.

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

ÍNDICE

MEMORIA 2014

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

LA AGENCIA EN CIFRAS

MEMORIA AEPD 2014

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

1 CIUDADANOS MÁS Y MEJOR INFORMADOS

El Servicio de Atención al Ciudadano es el primer punto de encuentro entre la Agencia Española de Protección de Datos (AEPD) y quienes quieren obtener más información o resolver cualquier duda acerca del derecho fundamental a la protección de datos personales.

Este servicio se encuentra disponible a través de diferentes canales (presencial, telefónico, postal y electrónico) que se complementan para garantizar que el ciudadano encuentre en la Agencia un organismo cercano que responde a sus inquietudes.

La **página web** de la AEPD (www.agpd.es) ha mantenido desde su creación un amplio repertorio de información dirigida a los ciudadanos, incluyendo guías y herramientas de utilidad para conocer diferentes aspectos del derecho a la protección de datos y cómo gestionar la privacidad. En 2012 la Agencia puso en marcha la posibilidad de realizar consultas automáticas a través de un catálogo de preguntas frecuentes y de presentar consultas singulares a través de la Sede electrónica. Estas opciones se afianzaron en 2013, consolidándose en 2014 como una opción sencilla y eficaz de obtener información.

Avanzando en la consecución del objetivo de ofrecer información práctica y cercana para ciudadanos y responsables, la Agencia Española de Protección de Datos presentó en diciembre de 2014 el rediseño de su página web, mejorando y actualizando su estructura, añadiendo nuevos contenidos y aportando una navegación adaptada a dispositivos móviles. El objetivo de la AEPD era ofrecer tanto a ciudadanos como a organizaciones una visión más ágil y global de los proyectos que organiza o en los que participa la Agencia a través de una estructura intuitiva y una navegación simplificada. Durante 2014, se comenzó también a trabajar en la mejora progresiva del buscador interno de su página web.

El cambio de diseño estuvo acompañado del lanzamiento de una nueva sección llamada La Agencia, un espacio orientado a reforzar la transparencia y que permite conocer tanto la información organizativa e institucional de la AEPD como la actividad que desarrolla y la administración y empleo de los recursos públicos. A partir de la presentación de esta nueva sección, la Agencia Española de Protección de Datos atiende en su propia web las obligaciones derivadas del principio de publicidad activa requeridas por la Ley 129/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, sin perjuicio de su participación en el Portal de la Transparencia como Unidad Singular, al ser un ente que actúa con plena independencia en el ejercicio de sus funciones.

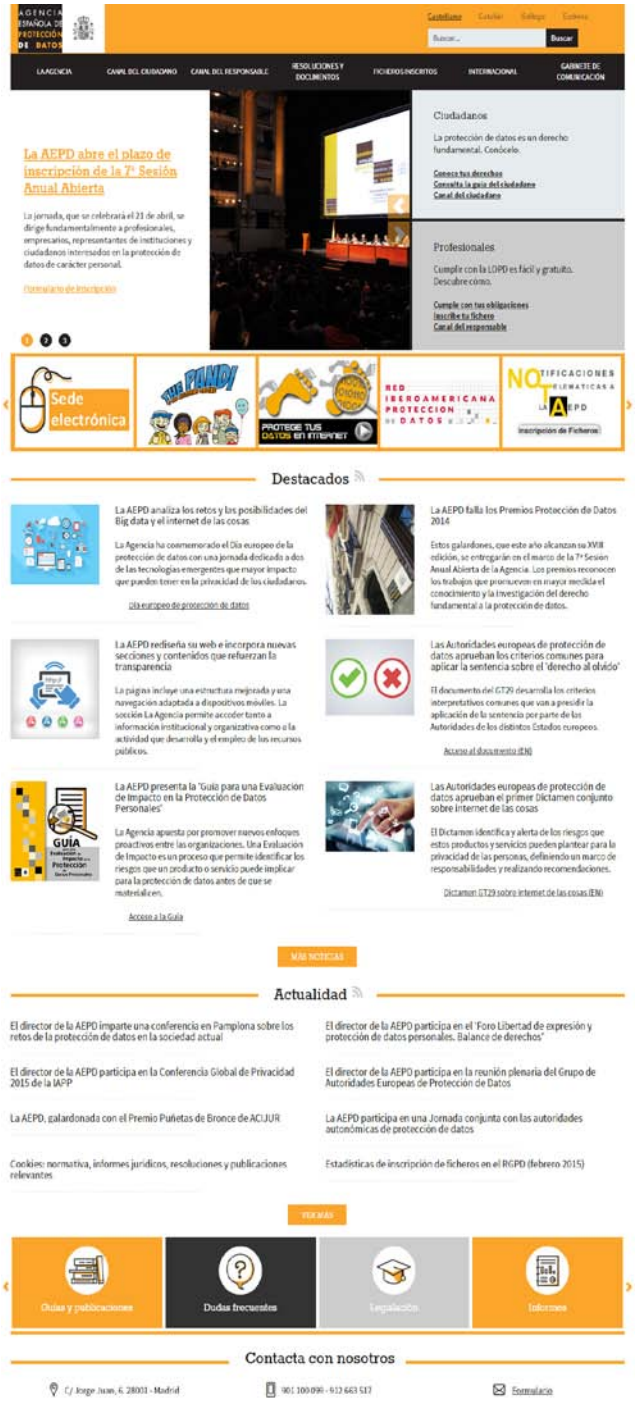
Los contenidos de la sección La Agencia están estructurados en cuatro grandes áreas: Información institucional y organizativa, Gestión económico financiera, Recursos humanos y Datos de interés. A estos espacios se añaden tres secciones adicionales que recogen los premios concedidos por la institución, la actividad de la AEPD y un formulario para todos aquellos ciudadanos que deseen solicitar información adicional. Este formulario se suma a los procedimientos electrónicos que ya estaban habilitados en la Sede electrónica de la Agencia, y que permiten desde la presentación de denuncias

o reclamaciones a la consulta de solicitudes, quejas o sugerencias.

Continuando con las herramientas de mejora y ampliación de los contenidos de la web de la Agencia, la AEPD incluyó en octubre de 2014 una nueva sección orientada a clarificar y facilitar el cumplimiento de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) en materia de cookies. Con el fin de convertirse en una herramienta de utilidad para los responsables de páginas web, esta página incluye una selección de la normativa aplicable en materia de cookies junto a los informes jurídicos, las resoluciones y las publicaciones más relevantes realizadas por la Agencia Española de Protección de Datos, así como documentos de interés elaborados por las Autoridades europeas de protección de datos.

Los accesos a la página web se aproximan a los seis millones (5.706.488) en 2014, lo que supone un incremento del 12,63% respecto al año anterior y un promedio de 7.816 visitas diarias frente a las 6.842 del año 2013. Asimismo, las herramientas disponibles en la web para los ciudadanos han visto incrementadas sus descargas. En concreto, el documento dirigido específicamente a promover los derechos de los ciudadanos, la *Guía del ciudadano: el derecho fundamental a la protección de datos,* sigue siendo uno de los documentos más consultados, con un incremento del 20,89% de las descargas realizadas, que han alcanzado la cifra total de 272.140.

Por su parte, el número total de **consultas** de ciudadanos atendidas ha ascendido a 198.378, de las que 94.821 corresponden a las planteadas a través de los canales tradicionales, 97.854 mediante la consulta automática al catálogo de preguntas más frecuentes y 5.703 a través de la Sede electrónica.



<Índice>

1

Mientras que el volumen de consultas a través de los canales tradicionales ha experimentado una ligera disminución del 3,71% con respecto a 2013, las realizadas a través de la Sede electrónica han aumentado un 22,99%, manteniéndose estable el volumen de consultas automáticas realizadas a través del catálogo de preguntas frecuentes. Estos datos ponen de manifiesto la creciente aceptación de los ciudadanos por mantenerse en contacto con la Administración utilizando los servicios electrónicos.

En relación con las consultas atendidas por vía telefónica (89.868), las más frecuentes han estado relacionadas con la inscripción de ficheros (24.657) y videovigilancia (4.007).

De las planteadas por escrito (6.295 consultas), tanto a través de medios convencionales (592) como a través de la Sede electrónica (5.703), destacan las relativas al ámbito de aplicación de la LOPD (837), a la cesión de datos (785), a los derechos amparados en la LOPD (634) y a la inclusión en ficheros de morosidad (599).

En cuanto a las consultas planteadas para recabar información sobre el ejercicio de los derechos (5.458), 3.008 corresponden al derecho de cancelación, 1.365 al derecho de acceso, 820 al derecho de oposición y 205 al derecho de rectificación. El incremento de las consultas sobre los derechos de cancelación (18,66%) y acceso (24,32%) constatan una tendencia creciente: que una de las mayores inquietudes de los ciudadanos es conocer qué informaciones personales son objeto de tratamiento y cómo evitarlo.

Por otra parte, de las 97.854 consultas que han realizado los ciudadanos a través del catálogo de preguntas frecuentes, 11.841 han estado relacionadas con los ficheros de morosos y recobro de deudas, 10.445 con la inscripción de ficheros y 9.655 con el ámbito de aplicación de la LOPD.

El elevado volumen de consultas sobre ficheros de morosidad debe relacionarse indudablemente con un entorno de crisis económica, con las importantes consecuencias negativas que supone la inclusión en los mismos y, también, con la incorporación indebida a dichos ficheros de personas víctimas de suplantación en la contratación de servicios básicos (como la telefonía o el suministro de agua y energía), que se analizan posteriormente en esta Memoria.

En relación con las consultas resueltas desde el Área de Atención al Ciudadano hay que destacar que el 99,81% fueron atendidas en un plazo inferior a 20 días, manteniendo el compromiso de seguir trabajando para alcanzar el 100%. Dada la importancia de este servicio, la Agencia realiza un seguimiento acerca del nivel de satisfacción de los ciudadanos. Para ello, como en años anteriores, se han realizado varias encuestas de satisfacción sobre la atención presencial y telefónica en el Área de Atención al Ciudadano. En este sentido, se puede concluir que prácticamente todas las personas que han accedido al servicio se encuentran satisfechas (99,7%) con la atención recibida, el contenido de la información, los conocimientos de quienes les atendieron y la corrección en el trato, un nivel de satisfacción superior al ya muy loable 97,4% de 2013.

Por su parte, el Registro General de la AEPD ha empezado a ofrecer en 2014 facilidades añadidas para que los ciudadanos puedan dirigirse a la Agencia por medios telemáticos. Este organismo se ha incorporado al Registro Electrónico Común (REC) y al Sistema de Intercambio de Registros (SIR) automáticos entre todas las Oficinas de Registro de la Administración General del Estado,

<Índice>

accesible a través del Portal de Administración Electrónica.

El Sistema de Interconexión de Registros es la infraestructura básica que permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas de forma segura y con conformidad legal, independientemente de la aplicación de registro utilizada siempre que esté certificada en la Norma SICRES 3.0.

La implantación de SIR permite eliminar el tránsito de papel entre Administraciones, aumentando la eficiencia y eliminando los costes de manipulación y remisión del papel, gracias a la generación de copias auténticas electrónicas de la documentación presentada en los asientos de registro.

- DIFUSIÓN DE ACTIVIDADES Y MEDIOS DE COMUNICACIÓN

La difusión que realizan los **medios de comunicación** del derecho a la protección de datos se ha convertido en los últimos años en un elemento esencial tanto para fomentar la sensibilización y el conocimiento de los ciudadanos en esta materia como para que los responsables cumplan con sus obligaciones legales. Continuando con la línea iniciada en años anteriores, la Agencia ha mantenido entre sus prioridades la atención personalizada a

los medios de comunicación, que han contribuido de forma imprescindible a divulgar la labor realizada por la Agencia Española de Protección de Datos, convirtiéndose en una piedra angular para que los ciudadanos perciban a este organismo público como garante de su derecho fundamental.

El Gabinete de comunicación ha atendido casi 400 solicitudes de información realizadas por los medios en 2014. En el ámbito de la comunicación proactiva, hay que destacar más de medio centenar de notas de prensa, convocatorias y notas de agenda informativa realizadas. A ello se suma la realización de informes en profundidad sobre materias de especial relevancia y la gestión de más de 70 tribunas y entrevistas concedidas por el personal de la AEPD.

En cuanto a la temática de las cuestiones planteadas, es necesario establecer un paralelismo entre estas y los retos que para el derecho fundamental a la protección de datos plantean los nuevos entornos tecnológicos. La videovigilancia, la contratación fraudulenta o la inserción indebida en ficheros de solvencia patrimonial y crédito siguen siendo materias objeto de consulta por parte de los medios de comunicación. Pero en paralelo, y posiblemente relacionadas con los estudios, dictámenes y guías publicadas por la Agencia, hay que mencionar las demandas de información relacionadas con las nuevas tecnologías y su impacto en la protección de datos. Algunas de ellas son las siguientes:

- Sentencia del Tribunal de Justicia de la Unión Europea sobre el denominado derecho al olvido, mediante el ejercicio de los tradicionales derechos de cancelación y oposición aplicados a los buscadores en internet: régimen de responsabilidades y pasos que deben seguir los ciudadanos para ejercer sus derechos, garantías a las libertades de expresión e información en la Red y criterios comunes de las Autoridades europeas de protección de datos.

- Análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles organizado por la Red Global de Control de la Privacidad con la participación de la AEPD.

- Primer dictamen conjunto sobre Internet de las Cosas por parte del Grupo de Autoridades europeas de protección de datos: responsabilidades y recomendaciones.

- Utilización de drones para la captura, recogida y tratamiento de datos personales: riesgos para la privacidad.

- Tramitación del Reglamento europeo de protección de datos: garantías añadidas y plazos para su aprobación.

- Nuevo sistema de notificación de quiebras de seguridad para los sujetos obligados.

- Cookies y otras tecnologías de seguimiento y monitorización online: orientaciones, garantías y obligaciones.

- Difusión de imágenes de terceros sin consentimiento en redes sociales y otros servicios de internet.

- Sentencia del Tribunal de Justicia de la Unión Europea por la que se declara inválida la Directiva de conservación de datos 2006/24/CE.

A estas solicitudes de información adicional hay que añadir las acciones de comunicación específicas llevadas a cabo por la Agencia, relacionadas en gran medida con la celebración de eventos y la presentación de proyectos de largo recorrido:

<Índice>

• Canal de vídeos «Protege tus datos en internet»

El 28 de enero de 2014 la AEPD presentó su canal de vídeos «Protege tus datos en Internet» (www.agpd.es/protegetuprivacidad), un proyecto online que ha contabilizado 116.257 accesos en su primer año. Incluye diez vídeos didácticos en formato de videotutorial en los que se explica, paso a paso, cómo configurar las opciones de privacidad de los principales navegadores, redes sociales y sistemas operativos móviles. El sitio pretende concienciar al ciudadano de que cuando navega por internet deja unas huellas digitales que otros pueden seguir, obteniendo información sobre aspectos relevantes de su vida. Pero también ofrecer soluciones para controlar y reducir ese rastro evitando, por ejemplo, que el perfil en redes sociales esté visible para todo el mundo o sea indexado por los buscadores, que el dispositivo móvil envíe información sobre su ubicación o que se pueda acceder a los datos almacenados en el terminal si este se perdiera o fuera robado.

La presentación del canal de vídeos de la AEPD coincidió con la celebración del Día Europeo de Protección de Datos.

• 6ª Sesión Anual Abierta de la AEPD

El 14 de marzo se celebró la 6ª Sesión Anual Abierta de la AEPD en el Teatro Real de Madrid. El evento, al que acudieron en torno a 1.200 expertos, tiene como objetivo servir como punto de encuentro entre la Agencia y múltiples sectores empresariales y sociales para dar respuesta a sus inquietudes. La Sesión Anual fue el marco escogido para presentar un borrador de la *Guía para una Evaluación del*

Impacto en la Protección de Datos (EIPD), una herramienta diseñada para evaluar los posibles riesgos que un producto o servicio puede implicar para la privacidad de las personas, permitiendo identificar y eliminar o mitigar esos peligros antes de que se produzcan.

- **Entrega de los Premios Protección de Datos 2013 (XVII edición)**

Durante la celebración de la 6ª Sesión Anual Abierta tuvo lugar la entrega de los Premios Protección de Datos correspondientes a 2013 en las categorías de Comunicación e Investigación, reconociendo así la difusión que realizan periodistas, medios de comunicación e investigadores de este derecho fundamental.

De un total de 39 candidaturas presentadas, el jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio de comunicación *ex aequo* a las periodistas Marimar Jiménez, de *Cinco Días* –por sus trabajos relacionados con la protección de datos dedicados, entre otros aspectos, a los cambios en la política de privacidad de Google o la ciberseguridad– y a Beatriz Navarro, de *La Vanguardia,* por sus informaciones relacionadas con la privacidad y la protección de datos, en las que abordó temas como el «derecho al olvido» o el nuevo marco europeo de protección de datos. En esta categoría de comunicación el jurado otorgó un accésit a la periodista Carmen Jané por sus artículos publicados en *El Periódico de Cataluña* relacionados con las nuevas amenazas contra la privacidad o las cookies.

En la categoría de Investigación, el jurado concedió el premio en su modalidad de trabajos originales e inéditos a Vicente Guasch por su trabajo *Las transferencias internacionales de datos en la normativa española y comunitaria,* mientras que se otorgó el accésit dentro de la misma modalidad a Ana Sánchez por su trabajo *Catálogo de buenas prácticas de seguridad informática del personal sanitario.* En la modalidad de investigación sobre trabajos originales e inéditos que tratan acerca del derecho a la protección de datos en países iberoamericanos, el jurado premió a la candidatura *Glosario Iberoamericano de Protección de Datos,* de Dolores Dozo y Pablo Martínez.

- **Curso «Protección de datos y nuevas tecnologías»**

La AEPD organizó durante las Actividades de Verano 2014 de la Universidad Internacional Menéndez Pelayo el curso *Protección de datos y nuevas tecnologías,* que se impartió entre el 30 de junio y el 4 de julio en el Palacio de La Magdalena de Santander. El seminario analizó el impacto y los retos que las nuevas tecnologías y los servicios de internet plantean en relación con el derecho a la protección de datos de carácter personal, abordando en profundidad diferentes cuestiones relacionadas con el denominado derecho al olvido, la aplicación de la normativa de cookies o el creciente fenómeno del Big Data. El curso dedicó también un amplio espacio a exponer las claves del futuro Reglamento europeo de protección de datos, así como a las evaluaciones de impacto, un instrumento para trabajar de forma preventiva sobre los posibles riesgos que puede plantear para la privacidad un producto o servicio.

- **Presentación «Guía para una Evaluación de Impacto en la Protección de Datos personales»**

A finales de octubre de 2014, y después de someter a consulta pública durante seis semanas una versión preliminar del texto, la Agencia presentó la versión definitiva de la *Guía para una Evaluación de Impacto en la Protección de Datos personales* en un acto en el participaron destacados representantes

<Índice>

tanto del sector público como privado. La publicación de esta guía –cuyo contenido se detalla en otro apartado de la Memoria– y el hecho de haber tenido en cuenta los comentarios y sugerencias recibidas para la redacción final de la misma, supone diseñar un marco de referencia flexible contando con la voz de unas organizaciones que, más allá del mero cumplimiento normativo, también deben asumir un compromiso activo y responsable con la protección de datos.

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 2014 finalizó con un total de 3.746.930 ficheros inscritos en el RGPD, cifra que supone un incremento de un 11% respecto al cierre del año anterior. De ellos, 3.594.106 ficheros son de titularidad privada (95,92%) y 152.824 de titularidad pública (4,07%).

La presentación de notificaciones a través de internet supone ya el 88,72% del total y sólo el 11,28% restante se realiza en formato papel. Asimismo, sigue incrementándose el uso de la firma electrónica en la presentación de notificaciones, que ha aumentado un 18% con respecto al año anterior, representando un 43,84% del total. De igual forma la notificación de las resoluciones de inscripción registral a través del sistema de Notificaciones Telemáticas (SISNOT) se ha incrementado en más de un 40% con respecto a las realizadas en 2013.

El número total de ficheros privados inscritos en 2014 se ha incrementado en un 11,31% con respecto a 2013 y el crecimiento del número de entidades del sector privado que tienen inscritos ficheros en el RGPD, es decir, responsables de ficheros, es de casi un 12% frente al 11% que se registró en 2013, lo que indica una mejora del nivel de cumplimiento de la LOPD en el sector empresarial español.

Si nos detenemos en las finalidades de los ficheros de titularidad privada inscritos durante 2014 en el RGPD, los que tienen por finalidad la «Gestión de clientes, contable, fiscal y administrativa» constituyen el mayor número de inscripciones y son los que representan el mayor volumen, suponiendo el 59% del total de ficheros privados. Destacan también los ficheros cuyas finalidades son las de «Recursos humanos», «Gestión de nóminas» y «Publicidad y prospección comercial». Mención especial merecen los ficheros cuya finalidad es la de «Comercio electrónico», aun cuando su número total no suponga más que un 2,79% del total de ficheros inscritos –pues el 25% de los mismos se ha inscrito durante 2014–, apuntando el desarrollo de este sector económico. Igualmente destacan, por su incremento, los ficheros que declaran tener por finalidad la de «Videovigilancia», al igual que en 2013, y la de «Análisis de perfiles», con casi un 19% y más de un 17%, respectivamente.

Por sectores de actividad, el mayor número de ficheros inscritos corresponde a los de las «Comunidades de propietarios» y «Comercio». Debe destacarse el incremento de los ficheros a nombre de «Organizaciones empresariales y profesionales», que en 2014 ha supuesto más del 25% del total de los ficheros inscritos a nombre de estos responsables. En este ámbito también hay que mencionar el crecimiento en el número de ficheros inscritos de entidades cuya actividad es la de «Comercio y servicios electrónicos», que ha sido superior al 20% aun cuando el total de los ficheros de estos sectores de actividad no represente, hasta el momento,

un volumen significativo en relación con el total de los ficheros privados.

El número total de ficheros de titularidad pública inscritos a finales de 2014 fue 152.824, lo que supone un incremento de un 4,8% sobre el año anterior frente al 6,5% que se produjo en 2013 con respecto a 2012. Esta disminución en el crecimiento sobre el total de ficheros públicos refleja que la adecuación de los responsables al cumplimiento de la LOPD se está consolidando. Por su parte, el incremento en el número de ficheros inscritos corresponde fundamentalmente a la Administración Local, que ha supuesto casi el 75% de las altas realizadas y representa ya el 58% del total de los ficheros públicos.

En lo que corresponde a la Administración General del Estado (AGE), el Ministerio de Hacienda y Administraciones Públicas ha incrementado su número de ficheros inscritos en un 65%, alcanzando un total de 1.000. Este crecimiento tiene su origen en la publicación, con fecha 1 de enero de 2014, de la Orden Ministerial en la que se incluyen todos los ficheros del Departamento y que ha venido a completar los tratamientos realizados, sobre todo, en las Delegaciones y Subdelegaciones del Gobierno de todas las Comunidades Autónomas y Provincias.

Con respecto a las Administraciones de las Comunidades Autónomas, el número total de ficheros inscritos ha seguido dos tendencias en clara continuidad con el anterior ejercicio que tienen su origen en las labores de puesta al día y reorganización: una representada por la Comunidad de Madrid, que decrece y que ha supuesto una disminución de más de un 9% en los ficheros inscritos de esta Administración; y la otra representada por las Comunidades Autónomas de Aragón y Extremadura, que incrementan su número de ficheros en casi un 13% y un 10%, respectivamente.

En la Administración Local ha aumentado el número de responsables que notificaron sus ficheros, donde la provincia de Segovia, con un incremento de un 133% destaca especialmente seguida de Cuenca con un 24%, Málaga, con un 11%, y Valladolid con un incremento de un 10%. En cuanto al crecimiento en el número de ficheros inscritos hay que mencionar de nuevo la provincia de Segovia, que amplía el número de sus ficheros en un 244%, seguida de Málaga con un 30%, y Cuenca y Zaragoza con un 24% cada una.

Las herramientas EVALÚA y DISPONE, que la AEPD ofrece a través de su página web para evaluar el cumplimiento de la LOPD y de las medidas de seguridad y ayudar a la elaboración de la disposición general de creación, modificación o supresión de ficheros de titularidad pública, respectivamente, siguen demostrando su utilidad para los responsables de los ficheros. Esto se refleja en que no sólo se mantiene el número de accesos a las mismas, sino que se incrementa el número de informes obtenidos de cada una de ellas.

A estas utilidades hay que sumar las guías dirigidas a facilitar información sobre el cumplimiento de obligaciones en relación con materias concretas, como la *Guía de videovigilancia, 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 de las tecnologías RFID,* la *Guía del responsable de ficheros* y la nueva *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD).*

En 2014 una de las guías más utilizadas por los ciudadanos, la *Guía de videovigilancia,* se ha actualizado y completado con seis fichas sobre in-

formación general de videovigilancia y específica en comunidades de propietarios, establecimientos públicos y control empresarial.

Los siguientes datos muestran la acogida de estos servicios en el ejercicio 2014:

- El formulario NOTA ha tenido 316.904 accesos para notificar ficheros a la Agencia.
- Se han solicitado 10.327 copias de contenido de ficheros.
- 9.202 usuarios han realizado el test EVALÚA LOPD.
- 3.005 usuarios han realizado el test EVALÚA SEGURIDAD.
- Se ha accedido en 4.876 ocasiones a la herramienta DISPONE, que permite preparar la disposición general de regulación de ficheros públicos.
- La Guía del responsable de ficheros y la Guía de seguridad, que se complementan para ofrecer orientaciones generales sobre el cumplimiento de la LOPD, han sido consultadas y/o descargadas en 90.462 y 71.252 ocasiones, respectivamente.
- El modelo de documento de seguridad ha sido descargado en 139.638 ocasiones.

El resto de las guías dirigidas a responsables del tratamiento han tenido el siguiente número de descargas:

- *Guía sobre el uso de las cookies:* 390.460.
- Guía *La protección de datos en las relaciones laborales:* 310.548.
- *Guía para clientes que contraten servicios de Cloud computing:* 264.974.
- *Orientaciones para prestadores de servicios de Cloud computing:* 61.637.
- *Guía sobre seguridad y privacidad de las tecnologías RFID:* 160.351.
- *Guía de Videovigilancia:* 107.985 ocasiones.
- La *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD):* 152.821 descargas.

<Índice>

Los datos sobre descargas en este ámbito ponen de manifiesto una estabilización en el uso de las herramientas y guías que facilitan el cumplimiento de las obligaciones genéricas de la LOPD y un notable incremento del de las guías que ofrecen soluciones prácticas para la aplicación de dicha norma a tecnologías que están alcanzando un ritmo creciente de desarrollo como los servicios de Cloud computing, las cookies o las tecnologías RFID. Este crecimiento se aprecia también respecto de las guías sobre videovigilancia, posiblemente asociado al crecimiento constante de esta actividad en el sector privado, y sobre la guía y el modelo de seguridad.

Asimismo, es muy destacable el importante número de descargas de la *Guía para una Evaluación de Impacto en la Protección de Datos Personales* que, pese a ser editada el 29 de octubre de 2014, ha ascendido a más de 150.000 en sólo dos meses, lo que parece indicar un alto interés y una mayor sensibilización por los modelos preventivos de cumplimiento de la normativa de protección de datos.

En otro ámbito, la LOPD prevé la adopción de **códigos tipo**, o códigos de conducta, como fórmulas de autorregulación que permitan a sectores de actividad, empresas, administraciones o corporaciones públicas adecuar el cumplimiento de la normativa a sus características específicas.

Durante 2014 se acordó la cancelación de la inscripción en el Registro General de Protección de Datos del código tipo denominado «Código Tipo Veraz-Persus» con código de inscripción CT/00001/2006, a solicitud de su promotor Soluciones Veraz Asnef-Equifax, S.L.

Asimismo, se han presentado formalmente dos solicitudes de inscripción de códigos tipo:

- «Código Tipo de Protección de Datos Personales del Fichero Asnef Protección», promovido por la Asociación Nacional de Entidades de Financiación (ASNEF), cuyo precedente se encuentra en el código tipo cancelado, pendiente al finalizar el año de dictarse la correspondiente resolución sobre su inscripción[1].

- «Código Tipo del Tratamiento de Datos de Carácter Personal aplicable al tratamiento de datos de las Oficinas de Farmacias del Colegio de Farmacéuticos de Barcelona», presentado el 2 de diciembre de 2014 y cuyo promotor es el Colegio Oficial de Farmacéuticos de Barcelona. Su tramitación se realiza en colaboración con la Autoridad Catalana de Protección de Datos al incluir en su ámbito objetivo de aplicación tratamientos de datos competencia de dicha Autoridad.

En 2014 han finalizado las labores de orientación para la elaboración de códigos tipo con la Federación Nacional de Clínicas Privadas (FNCP) y otras asociaciones sanitarias privadas, y con la Asociación Nacional de Entidades de Gestión de Cobro (ANGECO), cuya presentación formal se debería producir en 2015.

Además, se han iniciado labores de orientación dirigidas a la modificación y adecuación a la normativa de protección de datos de tres códigos tipo inscritos en el RGPD. Se trata de los siguientes: «Código Tipo de La Unió Catalana D´Hospitals», promovido por Unió Catalana d´Hospitals; «Código Tipo del Fichero Histórico de Seguros del Automóvil»; y «Código Tipo del Fichero de Automóviles de Pérdida Total, Robo e Incendios», promovidos ambos por UNESPA.

[1] Se ha inscrito el 21 de enero de 2015.

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 528, de las cuales 334 (63%) fueron planteadas por las Administraciones Públicas y 194 (37%) por el sector privado.

Se produce así un incremento del 8% en el volumen de consultas planteadas respecto a las formuladas el año anterior, que fueron similares a las de los años 2011 y 2012 y que implicaban una reducción frente a las formuladas en los años inmediatamente posteriores a la entrada en vigor del RLOPD y, en particular, a los años 2008 a 2009. De este modo, las cifras del ejercicio 2014 se asemejan a las existentes con anterioridad a la entrada en vigor del RLOPD, si bien cabe apreciar que en este ejercicio 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 poco después de la aprobación del citado RLOPD.

Igualmente se aprecia, en cuanto al reparto de las consultas de los sectores público y privado, la mayor preponderancia de las procedentes del sector público (que en este ejercicio ya alcanzan el 63% del total), manteniéndose la tendencia mostrada en ejercicios posteriores (cabe recordar que en el año 2013 las consultas del sector público representaban un 65% del total, cifra relativamente similar a la de este año).

De las **materias objeto de consulta** cabe extraer las siguientes conclusiones:

- El mantenimiento de un 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 2014 ascendieron a un total de 16, manteniéndose así una cifra similar a la del ejercicio anterior.

- La aparición, fundamentalmente en el último tramo del año, de un número relevante de consultas relacionadas con la aplicación de los principios de protección de datos en las materias reguladas por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

- El notable crecimiento de las consultas relacionadas con la prestación de servicios de la sociedad de la información y los tratamientos de datos llevados a cabo en el ámbito de internet. Así, las consultas relacionadas con estos servicios se incrementaron en un 150% en 2014, pasando de 10 a 25. Igualmente, las cuestiones relacionadas con la aplicación de la normativa relacionada con la instalación de dispositivos de almacenamiento masivo en los terminales de los usuarios, tales como cookies, se incrementaron desde una única consulta en 2013 a 9 en 2014.

- El novedoso incremento de las cuestiones relacionadas con la videovigilancia, que habían descendido progresivamente en anteriores ejercicios, debido posiblemente a la aprobación de la Ley 5/2014, de 4 de abril, de Seguridad Privada. Estas consultas se incrementaron en un 85% en el año 2014.

- El aumento de las consultas relacionadas con conceptos generales de la LOPD y su ámbito de aplicación (incrementos del 66% y el 23% respectivamente), así como 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 de datos, produciéndose un in-

<Índice>

crecimento del 19% que debe añadirse al que ya se dio en 2013 (de un 74% respecto del 2012). También es relevante el incremento en un 21% de las consultas relacionadas con ficheros de titularidad pública.

- El mantenimiento de un número relevante de cuestiones relacionadas con las cesiones de datos (manteniendo un volumen superior al 35%), siendo igualmente relevante el número de cuestiones relacionadas con los requisitos para la prestación del consentimiento (un 17% del total).

- El moderado descenso de las cuestiones relacionadas con las medidas de seguridad (un 18%) y la normativa de telecomunicaciones (un 22%).

- El muy notable descenso de las consultas relacionadas con los ficheros de solvencia patrimonial y crédito (un 60%) y el padrón municipal de habitantes (un 78%).

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

- El notable incremento de las consultas planteadas por las entidades dedicadas a la prestación de servicios de asesoría y consultoría, invirtiendo la tendencia de ejercicios anteriores. Es preciso recordar en este punto el criterio de la Agencia de atender únicamente las consultas relacionadas con sus ficheros y tratamientos y no con las de sus clientes, que deberán formularse por estos últimos. No obstante, la mayor parte de las consultas se referían a los tratamientos llevados a cabo por las propias entidades, bien como responsables bien como encargadas del tratamiento.

- El mantenimiento de las consultas realizadas por particulares, que siguen siendo las más abundantes dentro del sector privado, representando un 14% de las mismas. El incremento en este grupo de consultas es del 22% respecto de 2013.

- La relevancia de las consultas formuladas por las empresas de seguridad privada, que ascienden a un total de 8, sin que constase ninguna consulta planteada en el ejercicio anterior.

- El notable aumento de las consultas procedentes de los sectores de distribución (de un 367%), y telecomunicaciones (de un 44%). Por otra parte, vuelven a incrementarse las consultas del denominado tercer sector (en un 56%), aunque sin alcanzar las cifras que se registraron en 2013.

- La disminución de las consultas realizadas por los sindicatos y partidos políticos (33%), y las asociaciones empresariales y profesionales (43%). Asimismo se produce un descenso en los sectores sanitario (46%), industrial (54%) y de los ficheros de solvencia patrimonial y crédito (56%). En particular, es muy significativo el descenso en un 87% de las consultas procedentes del sector energético.

- En el sector público se reduce el peso de las consultas formuladas por la Administración General del Estado, que desciende del 52% al 45%, por lo que en los dos últimos años su peso se ha reducido en 21 puntos porcentuales. Al propio tiempo, se incrementan en un 49% las consultas planteadas por Administraciones de las Comunidades Autónomas (que ya representan un 24% del total del sector público). También es relevante el aumento en la Administración corporativa e institucional (de un 32%), repre-

sentando ya estas consultas un 16% del total procedente del sector público.

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:

- La posible creación, al amparo del artículo 7.f) de la Directiva 95/46/CE, de sistemas de prevención del fraude de carácter multisectorial, siempre y cuando se adopten medidas reforzadas de minimización de la información que podrá ser compartida por las entidades participantes en estos sistemas. Igualmente, se analizaron cuestiones concretas relacionadas con los ficheros de carácter sectorial, cuya viabilidad ya había sido ratificada en el año 2013.

- La posibilidad de que por las Fuerzas y Cuerpos de Seguridad se faciliten a las entidades financieras datos referidos a las imágenes captadas por sistemas de videovigilancia en entidades de crédito, siempre que se trate de las referidas a acciones delictivas, con la finalidad de mejorar la reacción ante estos hechos, debiendo limitarse el acceso a las imágenes a una lista tasada de personas de sus departamentos de seguridad. Además, se implantaban en los accesos las medidas de seguridad de nivel medio.

- La posible publicación en la intranet del Ministerio Fiscal, al amparo del artículo 7.f) de la Directiva 95/46/CE de los currículos de los candidatos a plazas de designación discrecional de la carrera fiscal, siempre que se trate exclusivamente de datos profesionales y se informe expresamente de la prohibición de su uso posterior.

- La conformidad con lo dispuesto en el artículo 11.2 c) de la LOPD de la creación de una plataforma para intercambio por las entidades financieras de información de bastanteos de los poderes de quienes ostentan su representación de los clientes ante las mismas, siempre que los apoderados sean suficientemente informados sobre esta cesión.

- La necesidad de que quede acreditada la trascendencia tributaria de la información requerida por la Hacienda Pública en determinados supuestos. En particular, se hace referencia a la consulta formulada por un Juzgado de Primera Instancia al que se requerían datos de la totalidad de los procesos tramitados ante el mismo, incorporando no sólo los datos de los profesionales que participan (abogados y procuradores), sino también los de los interesados, tipo de procedimiento y cuantía litigiosa, o a la solicitud de datos relacionados con las intervenciones llevadas a cabo por un determinado facultativo. Por el contrario, se informó de que revestía trascendencia tributaria el suministro de información referida al consumo eléctrico por parte de los prestadores de este servicio, la cesión de datos relacionados con la enajenación de bienes del patrimonio artístico o la referida a las ventas efectuadas por comerciantes de objetos preciosos.

- La viabilidad del tratamiento de datos derivado de la creación de una aplicación móvil para el abono del estacionamiento vigilado y de las sanciones que pudieran imponerse. No obstante, se indicó que dicha aplicación no debería mostrar información sobre la localización de los vehículos, a fin de evitar su uso abusivo por terceros.

- La licitud de la cesión a los miembros de una asociación de la información referida a las cuentas de la misma y a la retribución de sus em-

<Índice>

pleados, al amparo de la ley Orgánica 1/2002 reguladora del derecho de asociación.

- La licitud, al amparo del artículo 11.2 c) de la LOPD, de la comunicación de datos personales entre compañías aseguradoras en supuestos de seguro múltiple para satisfacer el interés legítimo de obtener el recobro de las cantidades abonadas en exceso por alguna de las aseguradoras, siempre que se limite a los datos referidos a la cobertura del riesgo y al importe calculado de la indemnización que corresponde a cada asegurador.

- La inexistencia de legitimación para que una empresa de alquiles de vehículos pueda recoger el dato de la huella dactilar de sus clientes con el fin de prevenir la comisión de delitos, dado que la seguridad pública es competencia exclusiva el Estado, encomendada a Fuerzas y Cuerpos de Seguridad.

- La imposibilidad de considerar amparada en el artículo 7.2 de la LOPD la cesión de los datos de los afiliados a un partido político a uno de sus militantes o de un sindicato a una fundación creada por el mismo. Tampoco es conforme a la LOPD la publicación de los miembros de una hermandad religiosa, a menos que los hubieran hecho manifiestamente públicos.

- La licitud de la cesión por un colegio profesional de los datos de los beneficiarios del servicio médico prestado con anterioridad por el mismo a una mutua de seguros a prima fija creada para reemplazar dicho servicio médico, considerándose que, no obstante, no procedía la aplicación del artículo 19 del RLOPD, al no producirse realmente una subrogación entre ambas.

- La limitación del alcance del contenido de los partes justificantes de la solicitud de una licencia por enfermedad familiar, que deberán limitarse a indicar que concurren los requisitos legales, sin incluir la concreta dolencia padecida por el familiar.

- La atención de distintas consultas referidas a la aplicación de la excepción a la exigencia de medidas de seguridad de nivel alto prevista en el artículo 81.5 b) del RLOPD (tratamiento «incidental o accesorio» de datos especialmente protegidos). Así, no procede la exigibilidad de nivel alto en el caso de los datos de salud facilitados a un establecimiento de hostelería por los huéspedes, siempre que se proceda a su cancelación al concluir el hospedaje. Por el contrario, sí procede la aplicación de tales medidas en el caso de datos de salud asociadas a tarjetas de fidelización de un centro comercial para la realización de ofertas relacionadas con los mismos.

- La resolución de determinadas cuestiones relacionadas con la aplicación de la Ley 19/2013, de transparencia, acceso a la información y buen gobierno, planteadas antes de su entrada en vigor. En este sentido, durante ese período transitorio se indicó que era de aplicación el artículo 37 de la Ley 30/1992 en su redacción inicial, si bien interpretado a la luz de lo dispuesto en la nueva Ley. Asimismo se consideró procedente el acceso a la información de un expediente académico en caso de que el interesado pudiera alegar la existencia de una relación competitiva con el primero y el acceso por los progenitores a los expedientes de sus hijos mayores de edad. También se informó favorablemente el acceso a los datos de productividad solicitado por quienes participaban de la misma partida, considerándose improcedente el acceso a las firmas digitalizadas de los intervinientes en un

determinado convenio, al ser irrelevante para la finalidad de transparencia.

- La conformidad con la LOPD de la creación por un sujeto obligado en los términos de la Ley 10/2010 de prevención del blanqueo de capitales y la financiación del terrorismo de un fichero de personas con responsabilidad pública, conteniendo los datos de nombre, apellidos y número de identificación fiscal o pasaporte, así como, en su caso, la condición de familiar o allegado de la persona con responsabilidad pública y el tipo de acto o negocio del que deriva la condición de allegado. Igualmente se considera que la cesión de estos datos a otros sujetos obligados se encuentra amparada por el artículo 11.2a) de la LOPD, en conexión con el 15.1 de la Ley 10/2010. También en esta materia se ha informado favorablemente el acceso por sujetos obligados a la base de datos de titularidad real del Consejo general del Notariado, al amparo de los artículos 4 y 8 de la citada Ley 10/2010.

- La indicación, en relación con los ficheros referidos al cumplimiento o incumplimiento de obligaciones dinerarias, de que no resulta preciso que el responsable del fichero común notifique a los afectados la modificación de la identidad del acreedor en los casos de cesión de créditos, si bien será preciso que esta circunstancia haya sido informada por el cedente del crédito. También en este ámbito, se informó negativamente el establecimiento de un sistema de requerimiento de pago a través de la realización de llamadas automáticas, al no poder acreditarse su efectiva recepción por el deudor.

- La inaplicación de la LOPD en caso de imágenes captadas por cámaras cenitales que reproducen en tiempo real ubicaciones de distintas localidades desde una altitud considerable y no están dotadas de herramientas que permitan aproximar la imagen a los transeúntes. También se ha considerado amparada en el artículo 11.2 a) de la LOPD en relación con el artículo 16 de la Ley de contrato de seguro la cesión de los datos de un siniestro a la compañía aseguradora que ha de satisfacer la indemnización.

- La licitud de la cesión de imágenes captadas en el interior de transportes públicos municipales a la policía local cuando sea necesaria para prevención de un peligro real y grave para la seguridad pública o la represión infracciones penales y, en particular, en caso de que el conductor accione un dispositivo de emergencias establecido al efecto, se trate de grabaciones relacionadas con la comisión de un delito denunciado por un ciudadano, o cuando se detecte la comisión de un delito flagrante o se produzca la visualización en tiempo real en supuestos excepcionales de dispositivos policiales especiales ante un evento importante o amenaza, siempre que se adopten, en este caso, medidas adicionales de garantía de los derechos de los afectados.

- La inaplicación a los servicios de mensajería instantánea de la Ley 25/2007, de Conservación de datos en las comunicaciones electrónicas, al tratarse de prestadores de servicios de la sociedad de la información y no de operadores que lleven a cabo la explotación de una red pública de comunicaciones electrónicas.

- La legitimación de los partidos políticos concurrentes en un proceso electoral al tratamiento de los datos del censo electoral, conforme al artículo 41.5 de la Ley Orgánica 5/1985, si bien deberá procederse a la supresión de los datos al término de la campaña y únicamente podrán usarse los datos para los fines previstos en la propia Ley. No será posible el ejercicio del

<Índice>

derecho de oposición de los electores sobre la mera invocación de su deseo de no recibir propaganda electoral, al haber limitado la Ley los supuestos en que este derecho puede ejercerse. En todo caso, los partidos deberán ser responsables de un fichero, debidamente inscrito en el RGPD y relacionado con esta finalidad, aunque no será precisa la creación de un fichero diferente por campaña electoral.

- La aplicación a supuestos concretos de las previsiones contenidas en la Guía sobre el uso de las cookies, analizando en particular el alcance y contenido de la información que deberá constar en cada una de las capas que habrá de establecer el prestador de servicios de la sociedad de la información y poniendo de manifiesto los distintos supuestos en los que podría apreciarse que tal información es insuficiente a los efectos previstos en el artículo 22.2 de la LSSI.

- La aplicación de las reglas de la Ley 41/2002 para la viabilidad del consentimiento de los menores al tratamiento de sus datos personales en la historia clínica, aplicándose el mismo criterio para el acto médico que para el tratamiento asociado a aquél. Asimismo, se señaló que el menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica, pudiendo igualmente los datos ser cedidos a los titulares de la patria potestad del menor de edad sujeto a aquélla, mientras esa situación persista, para el cumplimiento de las obligaciones previstas en el Código Civil, sin que quepa oponer a ese acceso la oposición del menor salvo que así lo reconociera una norma con rango de Ley.

B) UNA RESPUESTA INTEGRAL A LAS NECESIDADES DE LOS CIUDADANOS

En 2014 se ha producido un nuevo incremento en el número de reclamaciones registradas tras la estabilización que se produjo en 2013. 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. El año 2013 supuso un ligero descenso del 1,70% motivado –a pesar del aumento del 0,15% en las denuncias– por una disminución del 8,94% en el número de escritos de reclamación de tutela presentados. En 2014 se ha registrado un incremento total del 14,80% en el número de reclamaciones presentadas (12.173), motivado por un crecimiento del 5,11% en los escritos de reclamación de tutela de derechos y, principalmente, por un incremento del 17,04% en el número de denuncias.

En definitiva, en cuatro años se ha producido un crecimiento del 81,6% en el número de reclamaciones presentadas, que se añade al ya producido en el periodo 2007-2010 de aproximadamente el 265%.

En cuanto a la resolución de las mismas, en el periodo 2013-2014 se ha producido un crecimiento del 4,48% (11.222 frente a 10.741 en 2013). Destaca también un incremento en el ejercicio de la potestad sancionadora (10,92%). Según el tipo de procedimiento incoado debe subrayarse el producido en la resolución de los procedimientos de apercibimiento (43,84%) y de los desistimientos (12,53%). En términos globales contrasta un incremento del 12,36% en las resoluciones de archivo de los diferentes procedimientos frente a una ligera disminución (0,23%) en las resoluciones declarativas de infracción, cifra motivada, en parte, por la

disminución en un 13,46% de las resoluciones de declaración de infracción de las Administraciones Públicas.

El elevado número de archivos –bien por resoluciones de inadmisión a trámite que aumentan un 11,30%, o de archivo tras actuaciones de investigación que crecen un 6,44%– también está motivado por las razones ya destacadas en años anteriores:

a) Inaplicación de la LOPD por diversas razones como:

– Estar el asunto excluido de su ámbito territorial de aplicación.

– Ser el afectado una persona jurídica.

– Realizarse tratamientos de datos relativos a fallecidos no amparados por la LOPD.

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

c) Falta de aportación por el denunciante de elementos mínimos que permitan realizar una investigación. Así, las denuncias por llamadas comerciales no consentidas no pueden ser investigadas si no se informa de la hora y minuto de las mismas ni de la titularidad de la línea telefónica que recibe las llamadas.

d) El carácter excepcional del procedimiento sancionador, que hace necesario analizar cuidadosamente si el ordenamiento permite otras fórmulas alternativas como el ejercicio de derechos de acceso, rectificación, cancelación y oposición, y la naturaleza de la infracción.

e) La falta de competencia de la Agencia atendiendo al ámbito territorial de aplicación de la LOPD, como ciertos casos relativos a directorios de internet que reproducen guías telefónicas desactualizadas, directorios profesionales o portales de contactos. La LOPD no resulta aplicable cuando sus responsables no tienen establecimiento en España desde el que se realicen tratamientos asociados a los servicios que prestan los sitios web ni utilizan medios en España.

f) La incorporación por el denunciado en fase de investigación de elementos probatorios que justifican archivar la denuncia (por ejemplo, la grabación de la conversación que acredita diligencia en la contratación o el pago de un número de facturas suficiente para interpretar que se ha prestado el consentimiento).

g) La aplicación de criterios jurisprudenciales que impiden la imposición de sanciones en determinados casos, como aquellos en los que no se prueba el contenido de las llamadas realizadas a familiares informando de la deuda o se completan datos no actualizados de los deudores por empresas de recobro.

Las resoluciones de procedimientos de apercibimiento han recaído de nuevo mayoritariamente en la actividad de videovigilancia (34,35%), debido a la habitual presencia como denunciados de particulares y pymes sobre los que procede aplicar los criterios de atenuación de la culpabilidad y antijuridicidad previstos en la LOPD en el caso de no haber sido sancionados o apercibidos previamente. No obstante, cabe destacar la novedosa adopción de 14 resoluciones de apercibimiento por comunicaciones comerciales electrónicas no consentidas tras la introducción de la figura en la Ley de socie-

<Índice>

dad de servicios de la sociedad de la información y de comercio electrónico por la disposición final 2.11 de la Ley 9/2014, de 9 de mayo. También destaca el crecimiento en el área de servicios de internet (78,95%) y en comunidades de propietarios (63,64%) en consideración a las infracciones que habitualmente se denuncian que, en el caso de que su gravedad no lo requiera, la agilidad y efecto reparador derivado de la incoación de un procedimiento de apercibimiento lo convierten en el instrumento legalmente más adecuado.

En lo relativo al volumen de las sanciones económicas declaradas, este disminuyó un 23,85% en 2014 a pesar de un incremento del 1,04% de las sanciones económicas impuestas, alcanzando la cifra de 17.330.345 euros.

Esta cantidad es consecuencia de una disminución del 5,37% en el número de sanciones graves impuestas y de la aplicación de los criterios de moderación y atenuación previstos en los apartados 5 y 6 del artículo 45 de la LOPD (66,50%).

Manteniendo la tendencia de años anteriores, y a pesar de la disminución respecto a 2013, el sector de actividad en el que se ha resuelto un mayor número de procedimientos (–17,77% con respecto a 2013) y se han declarado un mayor volumen de sanciones (–14,83% con respecto a 2013) ha sido el de las telecomunicaciones. Este descenso repercute en la disminución del importe total de sanciones declaradas (10.071.301 euros frente a los 15.035.008 euros de 2013). Este descenso está originado también por el efecto derivado de la invocación en mayor medida del «reconocimiento espontáneo de la culpabilidad» previsto en el apartado d) del artículo 45.5 de la LOPD como criterio de atenuación de la sanción.

Por el contrario, es llamativo el crecimiento de los procedimientos resueltos (67,57%) y de las resoluciones declarativas de infracción (58,06%) respecto a entidades financieras, así como respecto a empresas suministradoras de energía y agua (incremento del 16,67% y 8,33%, respectivamente). También destaca la subida en los procedimientos resueltos (11,94%) y de resoluciones declarativas de infracción (25,42%) respecto de la actividad de spam.

Las resoluciones más relevantes por áreas se detallan a continuación:

VIDEOVIGILANCIA

Desde el punto de vista cuantitativo, el mayor número de resoluciones sancionadoras se ha producido por la captación desproporcionada de la vía pública **(PS/00395/2014 y PS/00435/2014)** y por falta de cartel informativo sobre la actividad de videovigilancia **(PS/00098/2014).** En el ámbito de la videovigilancia se pueden destacar las siguientes resoluciones:

Cámaras en un instituto - E/04975/2013

Una trabajadora denunció a un centro educativo por la instalación de un sistema de cámaras. La dirección del centro había informado en numerosos claustros al personal y a la AMPA sobre la instalación del sistema de videovigilancia. En el proceso de instalación cumplieron con el deber de información estando a la espera del registro del fichero para proceder a ponerlo en funcionamiento. La ubicación de las cámaras era proporcional, limitándose sólo a pasillos y entradas al centro, y estas no se encontraban en funcionamiento por lo que no se acreditó tratamiento de las imágenes para usos diferentes a los informados.

Cámara en garaje - A/00044/2014

Un vecino denunció a otro por haber colocado una cámara de vigilancia en su plaza de garaje sin tener

autorización de la comunidad de propietarios. El denunciado no acreditó contar con la citada autorización y en las imágenes que aportaba de lo que captaba su cámara se apreciaba que excedía del espacio de su plaza de garaje, incluyendo elementos comunitarios y plazas colindantes. Se procedió a apercibir al denunciado.

- **Consecuencias laborales de la videovigilancia en trabajadores de seguridad - E/03357/2014**

La denunciante, empleada de una empresa de seguridad, manifestó haber sido sancionada por falta laboral grave, para lo que la empresa había utilizado y aportado en juicio las imágenes captadas por el sistema de videovigilancia del hospital en el que prestaba sus servicios sin que hubiera sido informada de que se utilizaban para el control laboral. De las actuaciones practicadas se constató que la implantación del sistema de videovigilancia, cuyo responsable era el hospital, tenía por finalidad la seguridad de las instalaciones y no el control laboral. La captación y utilización de las imágenes obedeció a fines de seguridad, detectándose a través de ellas un problema de este tipo provocado por la denunciante en su actividad laboral. La aportación de las imágenes por la empresa en el juicio como prueba de la conducta laboral de la denunciante y del riesgo de seguridad provocado con la misma está legitimada por el criterio jurisprudencial, según el cual «una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales, es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD). Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones». En consecuencia, se archivaron las actuaciones.

- **Cámaras de entidad bancaria que captan imágenes de la vía pública - PS/00303/2014**

De las actuaciones practicadas se comprobó que el sistema de la entidad denunciada captaba imágenes que excedían del ámbito o entorno privado, pues enfocaban a la vía pública. La entidad bancaria alegó que no trataba datos personales pues no vinculaba las imágenes captadas a personas físicas, argumento que no podía ser tenido en cuenta dado que las imágenes de personas constituyen datos de carácter personal y su captación implica su tratamiento. Aunque la normativa de seguridad privada obliga a las oficinas bancarias a instalar sistemas de videovigilancia, ello no ampara el tratamiento de imágenes de personas que transitan por la vía pública, que está reservado en exclusiva a las Fuerzas y Cuerpos de Seguridad. Por tanto, se produjo un tratamiento de datos sin consentimiento.

■ ALTA EN SERVICIOS SIN CONSENTIMIENTO

- **Falta de acreditación - PS/00030/2014**

La afectada denunció que una operadora había contratado una línea de telefonía móvil a su nombre sin su consentimiento. La denunciada aportó copia del CD con la grabación de la conversación, aunque no se pudo considerar como prueba de suficiente diligencia para acreditar la contratación ya que el único dato personal que constaba era el nombre (sin apellidos).

- **Acreditación válida - E/0574/2013**

El denunciante manifestó que una empresa mixta de aguas había realizado un cambio de titularidad incorporándole como titular de un contrato de suministro de agua sin su autorización.

<Índice>

La empresa aportó la solicitud de cambio de titular del suministro, en la que constaban los datos de tres intervinientes: el solicitante (denunciante), el representante y el propietario de la vivienda. Aportaba asimismo copia de los tres DNI, por lo que se consideró que se había adoptado la diligencia suficiente, como requiere la doctrina de la Audiencia Nacional.

- **Responsabilidad del comercial y de la empresa - PS/00668/2013**

Una empresa de distribución comercial trató los datos personales del denunciante sin su consentimiento para incorporarlos al formulario de un contrato de electricidad y gas y entregárselos a la empresa de suministro.

Esta realizó el tratamiento de los datos del denunciante al tramitar el contrato, efectuando un cambio de compañía sin obtener el consentimiento inequívoco del denunciante, emitiendo facturas con los importes correspondientes a esos contratos sin comprobar la veracidad de los datos ni la voluntad del titular de los mismos.

Se resuelve declarando la infracción tanto de la empresa comercializadora como de la responsable del suministro al no haber acreditado ninguna de las dos diligencias en la comprobación de la identidad de la persona que se da de alta.

INCLUSIÓN EN FICHEROS DE SOLVENCIA PATRIMONIAL

- **Inclusión en Asnef tras el pago de la deuda - PS/00384/2013**

A pesar de tener conocimiento del pago de la deuda se mantuvieron los datos del denunciante en un fichero de morosos hasta que fueron dados de baja a instancias del propio denunciante.

- **Falta de requerimiento previo a la inclusión del dato en ficheros de solvencia - PS/00675/2013**

Los datos personales del denunciante fueron incluidos en un fichero de morosos sin haber requerido previamente el pago de la deuda. Ni en las actuaciones previas de investigación llevadas a cabo ni en el procedimiento la entidad denunciada acreditó haber realizado dicho requerimiento, por lo que tampoco se habría llevado a cabo la advertencia de la posibilidad de incluir al denunciante en el fichero en caso de impago.

- **Inclusión en ficheros de solvencia de datos de una deuda objeto de arbitraje - PS/00072/2014**

Se impuso una sanción por la inclusión en ficheros de solvencia de una deuda objeto de reclamación ante la Junta Arbitral de Consumo (JAC), que finalmente dictó laudo concediendo la razón al denunciante. La entidad denunciada adujo que no tuvo conocimiento de la reclamación hasta la notificación del laudo, del que solicitó aclaración sin obtener respuesta, por lo que continuó con la gestión habitual de la deuda. Estas alegaciones no podían atenderse debido a que no sólo el denunciado les comunicó la presentación de su reclamación ante la JAC, sino que en el laudo se incluyeron las alegaciones efectuadas por la empresa. Los hechos constituyen una infracción del principio de calidad de datos, previsto en el artículo 4.3 de la LOPD en relación con el 29, que exige que los datos que se incorporen a cualquier fichero sean exactos y respondan con veracidad a la situación actual de los interesados. Además, el artículo 38.1.a) del RLOPD establece que para incluir una deuda en un fichero de solvencia deberá ser cierta, es decir, irrefutable e indiscutible, y en este caso la deuda fue objeto de impugna-

ción ante un órgano competente para resolver sobre su certeza, que había otorgado la razón al denunciante.

- **Venta de cartera de deudas canceladas - PS/00294/2014**

Una operadora de telefonía cedió su cartera de deuda en la que se incluía una deuda de la denunciante que había sido satisfecha con anterioridad. El operador de telefonía manifestó que no tuvo constancia del pago en su momento, por lo que una vez efectuada la reclamación procedió a recomprar la deuda y a cancelarla, reconociendo que dicha deuda no debería haberse cedido. Los hechos se sancionaron como una cesión de los datos de la denunciante a un tercero sin que exista habilitación legal para ello en los artículos 347 y 348 del Código de Comercio, que no exigen el consentimiento del deudor pero que no resultan aplicables al no existir una deuda cierta, vencida y exigible.

- **Cesión de crédito e inclusión en ficheros de solvencia sin notificación al deudor - PS/00316/2014**

Se denunció la inclusión por parte de la entidad cesionaria en un fichero de solvencia de una deuda que no existía y de la que no se había reclamado el pago previamente. En las actuaciones practicadas se constató que la denunciante figuraba como cliente de una operadora de telefonía con un saldo deudor que fue cedido. Constaba también una carta de las dos entidades dirigida a la denunciante en la que se le informaba de la cesión de su crédito, pero no que fuera remitida y, por tanto, conocida por la denunciante. Los hechos se consideraron una cesión de los datos de la denunciante sin su consentimiento y sin contar con habilitación legal.

- **Sanción por recobro de deudas al considerar que utilizan técnicas que vulneran la Ley de Protección de Datos - PS/00163/2014**

La AEPD ha entendido que algunas de las técnicas utilizadas por empresas de recobro para conseguir que las personas liquiden deudas pendientes vulneran el deber de secreto cuando se divulga de forma indebida la condición del deudor a terceras personas. Algunas de estas estrategias son la colocación de carteles en el buzón del deudor y en la puerta de su vivienda donde aparecen datos personales como el nombre y los apellidos del afectado.

La Agencia también ha declarado infracciones cuando se entregan tarjetas de visita por parte de los cobradores a vecinos y familiares de la persona a la que se quiere cobrar la deuda.

- PUBLICACIÓN EN INTERNET DE DATOS ESPECIALMENTE SENSIBLES

- **Publicación de fotos de un bebé - PS/00734/2013**

Varias fotografías de la hija de los denunciantes, un bebé de pocos meses de edad, se encontraban colgadas en la web de la denunciada. En la resolución se justificó la no aplicación del apercibimiento al considerar la naturaleza sensible de la información asociada a un bebé que aparecía desnudo en una de ellas.

- **Tratamiento de datos en un motor de búsqueda interno - PS/00178/2014**

La denunciante busca su nombre y apellidos en internet obteniendo como resultado el enlace a un sitio web del que no ha sido nunca usuaria y que incluye vídeos de contenido pornográfico. Las acciones que realiza el buscador interno de la página denunciada suponen un tratamiento de datos

<Índice>

del que es responsable el editor en la medida en que tiene la posibilidad de configurarlo para que no guarde las búsquedas anteriores y no sean indexadas por los buscadores generales. Los hechos constituyen un tratamiento de datos sin el consentimiento de la afectada y sin que se aprecie ninguna otra circunstancia que lo legitime.

- **Datos de guardias civiles en página web - PS/00480/2013**

En una página web apareció íntegra una resolución publicada a través de la intranet corporativa de la Dirección General de la Guardia Civil. Dicho documento contenía un listado de 28 páginas en las que se relaciona los DNI, nombre, apellidos y otros datos laborales y de formación de más de 900 guardias civiles.

TRATAMIENTO DE DATOS EN EL ÁMBITO EDUCATIVO

- **Fotos de alumnos en anuarios no divulgados externamente - A/00165/2013**

El Colegio indicó que se editaba cada año un anuario con algunas fotografías de las actividades que se habían desarrollado durante el curso, así como fotos de los alumnos agrupadas por cursos. En este caso, nos encontramos con la realización de una actividad vinculada al desarrollo de la función educativa del centro en la que se realizaba un tratamiento proporcionado de la imagen del menor que no desbordaba, en principio, el ámbito de divulgación del propio colegio y de la cual se había informado a los padres o tutores. En consecuencia, no se dedujo vulneración de la LOPD.

- **Inserción de vídeos en YouTube dentro del ámbito educativo - E/07111/2013**

En este expediente se aborda la cuestión de la divulgación de la imagen de un menor en la plataforma de vídeos YouTube como actividad vinculada al desarrollo de la función educativa de un centro.

La resolución señala que el requerimiento por parte de un docente para el tratamiento de la imagen de un menor en abierto en una plataforma como YouTube no puede considerarse habilitado por la Disposición Adicional vigesimotercera de la Ley Orgánica 2/2003, de 3 de mayo, de Educación, que sólo legitima el tratamiento de los datos personales de los alumnos que sean estrictamente necesarios para la función docente y orientadora. En consecuencia, sería contrario a la LOPD la indicación de los docentes a los alumnos para que estos publicaran cualquier tipo de pruebas académicas en un formato abierto.

En el caso concreto, sin embargo, no se probó la existencia de un mandato de los profesores de publicar vídeos en la plataforma en abierto y el alumno afectado había publicado los vídeos relativos a la actividad académica que se le solicitaba en un entorno privado y restringido de YouTube, por lo que la difusión de la imagen del menor no desbordó el ámbito del propio centro educativo. En consecuencia, la Agencia resolvió archivar las actuaciones de investigación.

- **Publicación en página web sin consentimiento - AP/00042/2013**

Un instituto publicó en su página web, en abierto y a la vista de cualquiera, los datos personales relativos a todos los profesores y alumnos del centro. En los documentos constaban los datos de nombre y apellidos de profesores junto con sus horarios de clase y su cargo, así como el número de D.N.I. o N.I.E., los nombres y apellidos, fecha de nacimiento, nacionalidad, país de estudios previos y situación laboral de alumnos; divulgación que se consideró desproporcionada.

INFRACCIONES EN MATERIA DE SEGURIDAD

• Venta de tableta sin haber borrado datos anteriores - A/00242/2013

Se accede por parte de terceros a datos personales del denunciante contenidos en una tableta comercializada por un establecimiento que no había procedido a eliminar dicha información antes de ponerla de nuevo a la venta. El dispositivo había sido inicialmente adquirido por el denunciante, que lo devolvió al establecimiento advirtiendo que contenía información personal. En las diligencias policiales consta reconocido por el imputado que el denunciante alertó de la información personal que contenía la tableta devuelta por el mismo. Asimismo, consta que el segundo comprador accedió a los datos personales del denunciante.

• Datos personales accesibles en internet - PS/00337/2014

Diferentes datos y documentos de personas inscritas en la bolsa de empleo de un colegio oficial se encuentran accesibles sin restricciones en la web de este organismo y a través del buscador Google, entre ellos el currículo de la denunciante. El colegio ha reconocido su responsabilidad y ha manifestado que se debió a un error del programa que se subsanó tan pronto fueron conocidos los hechos. La incidencia se produce por el incumplimiento de la obligación de establecer medidas de seguridad que impidan el acceso no autorizado a los datos personales, prevista en el artículo 9 de la LOPD, por no adoptar la debida diligencia. Por su parte, en el **PS/00384/2014** se accedía a través del buscador Google al currículum vitae del denunciante, que lo había enviado a la página web de una confederación comarcal, siendo accesible a terceros en una búsqueda realizada con su nombre y apellidos. El acceso a los datos personales es consecuencia de un insuficiente o ineficaz funcionamiento de las medidas de seguridad, incumpliendo el principio de seguridad de los datos.

COMUNICACIONES COMERCIALES

En 2014 se mantiene la tendencia creciente de los ciudadanos que optan por limitar la recepción de comunicaciones publicitarias utilizando las alternativas que les ofrece la lista de exclusión denominada Lista Robinson, gestionada por la asociación Adigital.

El número de usuarios registrados en la misma ascendió a 384.259 con un incremento del 10,73%. La opción elegida mayoritariamente ha sido la de oponerse a la recepción de llamadas telefónicas (39,16% del total), seguida de la negativa a la publicidad a través de SMS/MMS (20,80%) y de correo electrónico (20,70%). En cuarto lugar figura la oposición a la publicidad postal, con un 19,27% del total.

• Envío de carta promocional con datos procedentes de fichero ilícito PS/00291/2014

Recepción por correo postal de una invitación con los datos personales de la denunciante para asistir a un acto promocional. En la invitación se indica que la información utilizada para el envío publicitario procede de una entidad que ha de ser considerada como responsable del fichero y a la que, por tanto, le incumbe acreditar el consentimiento de la denunciante para el tratamiento de sus datos, lo que no ha efectuado.

• Envío de SMS comercial sin contar con autorización y sin incluir mecanismo de baja - PS/00743/2013

Un ciudadano pone en conocimiento de la AEPD la recepción en su teléfono móvil de publicidad no consentida por parte de una operadora pese a estar inscrito en la Lista Robinson desde hace varios

<Índice>

años. La entidad imputada ha incumplido la prohibición de enviar SMS comerciales al número de teléfono móvil del denunciante sin contar con el consentimiento previo y expreso del mismo para ello y sin ofrecerle un mecanismo de oposición al tratamiento de sus datos.

- **Recepción de llamadas telefónicas comerciales tras haber comunicado la oposición a recibirlas - PS/00196/2014**

Se denuncia la recepción de llamadas comerciales en dos líneas pertenecientes a un operador de telefonía por parte de un segundo operador al que los denunciantes habían manifestado por escrito su voluntad de no recibir más llamadas. El número de teléfono es un dato de carácter personal cuando, como en el presente caso, la operadora conocía también el nombre, apellidos, DNI y domicilio que constan en el escrito de oposición a recibir llamadas. El denunciado alega que la oposición se debería haber efectuado a través de la Lista Robinson y no mediante una comunicación que no indica dirección ni departamento. Sin embargo, esta debió ser atendida por la operadora sin que sea relevante que vaya dirigida a un departamento concreto.

- **Recepción de correos electrónicos después de haber solicitado la baja como destinatario - A/00130/2014**

Se denuncia la recepción de correos electrónicos comerciales después de haber solicitado al remitente la baja como destinatario. La dirección de correo electrónico según su configuración puede ser un dato de carácter personal cuyo tratamiento exige el consentimiento del afectado. En este caso, se constató la remisión de los correos electrónicos que contenían información y noticias sobre el sector vinícola y, por tanto, no son comerciales. Sin embargo, el remitente no acredita disponer del consentimiento del denunciante. De hecho, los correos se remitieron después de que este solicitara la baja.

- **Venta de base de datos de empresas con datos personales - PS/00302/2014**

Denuncia sobre la venta de una base de datos de empresas con la que se han realizado 12 campañas de marketing a través de correo electrónico. Se ha constatado que la base de datos contiene datos de carácter personal y que, aunque en el contrato de compraventa se afirma que proceden de fuentes de acceso público, tal extremo no puede acreditarse. Corresponde al vendedor denunciado, como responsable del tratamiento de los datos personales, acreditar que cuenta con el consentimiento de los afectados, lo que no se ha producido. Los hechos constituyen dos infracciones: una del artículo 6.1 de la LOPD, por tratar datos de carácter personal sin el consentimiento de los afectados, y otra del artículo 11.1 de la LOPD, dado que la venta de los datos supone una cesión para la que tampoco se dispone del consentimiento de estos.

COOKIES

Resulta relevante señalar la resolución de 20 procedimientos declarativos de infracción en materia de cookies tras la modificación de la Ley de servicios de la sociedad de la información y de comercio electrónico por el Real Decreto-Ley 13/2012, de 30 de marzo por el que se transpuso la Directiva 2009/136/CE que modificó la Directiva 2002/58/CE. Respecto a las infracciones detectadas en materia de cookies se ponen de manifiesto principalmente tres situaciones:

1. Cookies exentas - E/02978/2014

La finalidad ese tipo de cookies es la gestión de una sesión de usuario. El Dictamen 4/2012 del Grupo de Trabajo del artículo 29 sobre la exención del re-

quisito de consentimiento de cookies pone como ejemplo de uso exceptuado en su punto 3.1 el de «*… las cookies de sesión que se utilizan para rastrear las acciones del usuario en una serie de intercambios de mensajes con un proveedor de servicios de manera coherente*» siendo esta la finalidad de la cookie descargada en el procedimiento especificado, razón por la que se procedió al archivo de actuaciones.

2. Se utilizan cookies no exentas pero el editor del sitio no cumple con la obligación de informar.

Tal circunstancia puede producirse por varias razones:

2.a) No informa en ningún caso.

A/00212/2014 - El sitio web no proporcionaba información alguna ni en la página principal ni en la de condiciones de uso o en el aviso legal, por lo que se procedió a dictar resolución de apercibimiento para que el responsable del mismo adopte las medidas correctoras oportunas.

Por el contrario, durante las actuaciones previas en el **E/02976/2014** el responsable regularizó la situación incluyendo información detallada de la existencia y las finalidades de cookies de terceros, tanto en una primera como en una segunda capa de información, y con un enlace llamado «política de cookies». En aplicación de la interpretación que realiza la SAN 455/2011 de fecha 29/11/2013 sobre la figura del apercibimiento, se procedió a archivar el procedimiento.

2.b) El editor informa en el sitio web pero sin una primera capa y sin que la información adicional sobre cookies, que está en otra página, se identifique en la página principal como relativa a esta materia.

PS/0059/2014 - El portal utilizaba cookies analíticas de terceros sin informar en una primera capa. La web contaba con una política de privacidad accesible desde un enlace instalado en su página principal llamado «Aviso Legal/Política de Privacidad», donde había información sobre cookies, pero dicha información no resultaba directamente visible ni accesible para los usuarios, ni tampoco reconocible para estos, ya que la denominación del enlace no incluía ninguna indicación que permitiera asociar el documento al que dirige con información sobre cookies. Además, la información proporcionada resultaba incompleta. Se procedió a apercibir tras la entrada en vigor de la modificación de la LSSI que introdujo dicha figura, en congruencia con el principio de aplicación de la ley más favorable, archivándose finalmente al retirarse las cookies durante la instrucción del procedimiento.

2.c) El editor informa en una primera y segunda capa, pero la información es incorrecta.

A/00206/2014 - En cuanto a la primera capa se observa que sólo se informa del uso de cookies que responden a finalidades de analítica web, sin hacerse mención a las finalidades publicitarias. En la segunda capa debería informarse sobre el uso de cookies publicitarias con identificación del tercero al que están asociadas, sin que se hiciera ningún tipo de referencia al respecto. Tampoco eran operativos los mecanismos ofrecidos para desactivar o eliminar las cookies.

3. Las cookies no son instaladas por el editor, sino por la plataforma utilizada por este para desarrollar la página web.

PS/00320/2013 - Se sancionó la falta de información a los editores que utilizan el servicio Blogger para la creación de sus sitios web acerca del almacenamiento y uso de cookies analíticas y publicitarias por parte de Google. La instalación por defecto de cookies sin informar de ello a los editores que utilizan dicha plataforma conlleva que estos, al no tener

<Índice>

conocimiento de tal circunstancia, no puedan informar a su vez a los usuarios que acceden a dichos sitios web y supone que Google utiliza sin información previa los datos relativos a los hábitos de navegación de los usuarios en beneficio de su política empresarial y para los servicios de publicidad.

- OTRAS RESOLUCIONES RELEVANTES – SECTOR PRIVADO

Además de las resoluciones que se han reseñado agrupadas por epígrafes, se han dictado otras resoluciones relevantes respecto de responsables privados. Entre ellas se pueden destacar las siguientes:

- **Datos de empresarios - E/00522/2014**

Los datos del denunciante figuraban inscritos en el Registro Mercantil en calidad de administrador solidario de una empresa. De ello se infiere que dichos datos fueron objeto de publicación en el Boletín Oficial del Registro Mercantil y, por consiguiente, existía habilitación para el tratamiento por terceros sin que procediera solicitar la cancelación de los mismos al ser exactos y veraces.

- **Ofertas de empleo presuntamente falsas - PS/00459/2013**

Se sancionó a un particular que insertaba ofertas de empleo presuntamente falsas y las utilizaba para obtener datos personales de las víctimas e incitarles a realizar un ingreso de dinero a cambio del material para realizar el supuesto trabajo.

- **Convocatoria de junta de propietarios con relación de deudores expuesta en un tablón de anuncios accesible a terceros - A/00128/2014**

Una comunidad de propietarios expone en su tablón de anuncios la convocatoria de la junta de propietarios que incluye un listado de deudores. El denunciante aporta al expediente la declaración en sede judicial del expresidente de la comunidad, que reconoció que durante su mandato se publicó el listado de morosos en un tablón accesible a terceros. Asimismo, confirmó que estas convocatorias se realizaban mediante comunicación en los buzones y en el citado tablón, pero no acreditó que la publicación en el tablón de la convocatoria y el listado de deudores tuviese lugar ante la imposibilidad de notificarla a alguno de los vecinos.

La publicación de las convocatorias de juntas de propietarios que contengan un listado de deudores, sin haber observado las exigencias establecidas en la Ley 49/1960, de 21 de junio, de propiedad horizontal, en un elemento comunitario como el tablón de anuncios constituye una vulneración del deber de secreto. Se apercibe a la comunidad denunciada al concurrir las circunstancias previstas en el artículo 45.6 de la LOPD y se insta a que justifique la retirada de la convocatoria y del listado de deudores del tablón de anuncios.

- **Identificación inexacta del conductor de un vehículo con el que se cometió una infracción de tráfico - PS/00329/2014**

Se denuncia la recepción de notificaciones administrativas por infracciones de tráfico cometidas con un vehículo alquilado que el denunciante no ha conducido. De las actuaciones practicadas se constata que la empresa denunciada facilitó el DNI del denunciante, junto con el número de contrato de alquiler, a las autoridades de tráfico en cumplimiento de la obligación de identificar al conductor del vehículo con el que se cometió la infracción. También se constató que en el contrato de alquiler consta el número de DNI del denunciante asociado a los datos personales de una persona distinta, sin que se disponga de copia del DNI o del permiso de conducir de esta persona. Los hechos constituyen

una infracción del principio de calidad de datos, establecido en el artículo 4 de la LOPD, que exige que los datos sean exactos y puestos al día, atribuible a la entidad denunciada por no adoptar ninguna cautela para asegurarse de la exactitud de los datos que comunicaba a la autoridad de tráfico.

- ADMINISTRACIONES PÚBLICAS

  - **Infracción de la Dirección General de la Guardia Civil por no informar de la instalación GPS en sus vehículos - AP/00032/2013**

La Dirección General de la Guardia Civil incorporó un sistema de GPS a los vehículos de los agentes sin que se les hubiera informado previamente acerca de la finalidad de la recogida de sus datos y sin especificar si esos datos podían ser utilizados para el control laboral.

  - **Justificantes de baja sanitaria - AP/00038/2013**

Una diputación exigió en una circular que, para justificar las ausencias del trabajo sin baja, se aportara justificante médico en el que constara la patología y la prescripción. Se declaró la infracción al principio de calidad de datos que establece que *«sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido».*

  - **Datos incorrectos sobre el Sistema de Información de Schengen - AP/00046/2013**

El Ministerio de Asuntos Exteriores (MAEC) reconoció que el Ministerio del Interior le informó de la retirada del señalamiento en el Sistema de Información de Schengen (SIS) de una ciudadana extranjera que se había comunicado de forma automática a ese departamento ministerial el 2 de abril de 2011. No obstante, constaba acreditado que el 8 de septiembre del mismo año el Consulado español del país de la afectada denegó la solicitud de visado de la denunciante ignorando la retirada. El MAEC manifestó que la ciudadana solicitó visado en la Embajada de España en dos ocasiones posteriores, siendo denegadas porque continuaba figurando como persona no admisible, sin que se hubiera producido la actualización de la lista a la que acceden las Oficinas Consulares Españolas.

Varias resoluciones analizan los límites de que disponen las **Administraciones Públicas** para realizar la divulgación de datos vulnerando el deber de secreto.

  - **Expedición a terceros de recibos por parte de una diputación - AP/00048/2013**

El Servicio de Recaudación de una diputación provincial expidió a un tercero sin consentimiento de los afectados sendos duplicados de recibos del Impuesto de Bienes Inmuebles pertenecientes al alcalde y a la esposa de un concejal.

La diputación provincial confirmó haber expedido dichos duplicados, sin acreditar que dispusiera del consentimiento de sus titulares, ni aportar acreditación ni justificación alguna de la condición de interesados por parte de la persona a la que se hizo entrega de dicha documentación, manifestando, incluso, que desconocía a quién se entregó.

  - **Sentencia sin anonimizar - AP/00008/2014**

Se acreditó la divulgación en el anuario de Derecho Militar Disciplinario, accesible a través de internet, de multitud de sentencias de la jurisdicción militar sin haber anonimizado a los intervinientes. La denunciante había actuado como testigo en una causa, resultando punible la constancia de sus datos

<Índice>

personales asociados a determinados pleitos instruidos por vulneración del régimen disciplinario.

- **Divulgación del sueldo de una directora de museo - E/03613/2013**

Se denunció una posible vulneración del derecho fundamental a la protección de datos a través de un bando publicado en diversos medios de comunicación en el que se aludía a datos económicos relativos al coste mensual e indemnización de la directora de un museo. Se consideró que el bando se refería a datos veraces y de interés para la opinión pública del término municipal al referir el sueldo y demás percepciones recibidas por la denunciante en función de su cargo. Además, se la citaba con la inicial de su primer apellido y un apellido que dificultaba su identificabilidad, por lo que se trataría de una información veraz, de relevancia pública y no excesiva en la medida en que lo tratado se encontraba relacionado con hechos objeto de controversia en el término municipal. Tal información personal identificativa, no obstante, debería ser cancelada de la página web una vez que los datos dejaran de ser relevantes.

- **Publicación del listado provisional de candidatos a un plan de empleo municipal del que se deriva información sensible - AP/00016/2014**

Se publicaron en los tablones de anuncios y en la página web de un ayuntamiento los listados provisionales de admitidos y excluidos en una convocatoria para la contratación de personal de un plan de empleo municipal. El ayuntamiento manifestó que la publicación de dichos listados era uno de los trámites necesarios del procedimiento de selección y contratación de personal para que los candidatos pudieran comprobar si sus solicitudes han sido correctamente baremadas. Además, las solicitudes incluían un párrafo en el que los solicitantes prestaban su autorización para que se utilizaran los datos personales de la solicitud a efectos de su tramitación. Sin embargo, la convocatoria no preveía la publicación de listados provisionales de admitidos y excluidos de los que, además, se deducía información sensible, dado que entre los criterios de preferencia se incluían la situación de desempleo, la percepción de prestaciones de nivel contributivo o asistencial y las cargas familiares. Los hechos constituyen una infracción del deber de secreto por cuanto que se difundieron datos personales relativos a la renta familiar y la situación de desempleo de los candidatos.

- **No utilizar la opción de copia oculta (cco) en envío de correos electrónicos masivos - AP/00040/2013**

Resulta sancionable la remisión por parte de un ayuntamiento de un correo electrónico sin utilizar la función de copia oculta a los correos privados de sus trabajadores, recogiendo en la dirección de muchos de ellos sus nombres y apellidos.

- **Recomendaciones a la Dirección General de Tráfico para el correcto tratamiento de los datos del registro de vehículos - E/08050/2014**

Tras realizar actuaciones previas de inspección sobre determinados aspectos del tratamiento de datos en el Registro de Vehículos de la Dirección General de Tráfico (DGT), se formularon diversas recomendaciones al objeto de que el acceso a la información contenida en el mismo se limitara a personas y finalidades legitimadas. Estas recomendaciones fueron las siguientes: a) que la aplicación del informe telemático del vehículo que se expide a los ciudadanos no permita acceder desde la página web sin declaración de interés legítimo, y que se realice una revisión posterior de las solicitudes y se detecte a los usuarios que presentan un gran número de solicitudes u otras anomalías; b) que se realice un seguimiento, con los controles opor-

tunos, de las entidades de la Asociación Española de Leasing y Renting para que sólo accedan a la información de los vehículos de su titularidad y no a la de la totalidad del Registro; c) que la DGT establezca las medidas de índole técnica y organizativa que deben implantar las entidades públicas y privadas que tienen acceso al Registro de Vehículos e informe expresamente de ellas; d) que se incluya en el informe o certificado de cargas una cláusula de advertencia a los solicitantes para que no desvíen la finalidad para la que se solicitaron los datos; e) que se desarrolle completamente el documento de seguridad.

De los procedimientos relacionados con el incumplimiento de las medidas de seguridad, destacan los siguientes:

- **Quiebra de seguridad en la sede de la Dirección General de Tráfico - AP/00013/2014**

La quiebra de seguridad en la Sede electrónica de la Dirección General de Tráfico (DGT) ocasionó el acceso por parte de los denunciantes a los datos de otros conductores tras identificarse mediante su certificado electrónico personal. La DGT confirmó la detección y corrección de un fallo en el algoritmo de generación de *tokens* de sesión, que al parecer ocasionaba la generación de *tokens* duplicados, provocando en determinadas circunstancias la asignación indebida a un usuario de la identidad de otro que estuviera accediendo simultáneamente. La Agencia notificó las incidencias y la DGT procedió a corregirlas.

- **Informe médico enviado a persona distinta del interesado - AP/00001/2014**

En el expediente constaba que el denunciante estuvo ingresado en un centro hospitalario público y dado de alta con un informe provisional, pues el definitivo lo envía el hospital por correo, correspondiendo el que recibió a otra persona que también estuvo ingresada en dicho centro.

La Agencia declaró la infracción de la LOPD por la vulneración de las medidas de seguridad exigibles y del deber de guardar secreto.

- **Falta de medidas adecuadas para conservar y localizar documentación con datos personales - AP/00057/2013**

Solicitada la devolución de la documentación aportada por el denunciante para la tramitación de una solicitud por lesiones permanentes no invalidantes, se le responde que no existe ninguna documentación original en el expediente. De las actuaciones practicadas se pone de manifiesto que se produjo un problema en el sistema de archivo y conservación de la documentación que impidió su correcta localización pues, con posterioridad a que la AEPD iniciara sus actuaciones, fue localizada y puesta a disposición del interesado, lo que evidencia que la entidad denunciada no adoptó las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos.

- **Comunicado de prensa con datos de militantes de un partido político - AP/00012/2014**

El Partido Popular (PP) denuncia que la oficina de prensa del Grupo Parlamentario Socialista (GPS) en el Congreso ha difundido un comunicado sobre un caso de corrupción que incluye documentación con datos personales de varios militantes. En las actuaciones practicadas se constata que desde dicha oficina de prensa se distribuyó la documentación a los medios de comunicación.

La Agencia acordó la apertura de un procedimiento de declaración de infracción de Administraciones Públicas de acuerdo con el criterio que se venía

<Índice>

aplicando en diversos precedentes en relación con los grupos municipales y de conformidad con la doctrina de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional que establece que, con independencia de la naturaleza pública o privada de una asociación, si ejerce funciones públicas deberá considerarse responsable de tratamientos de naturaleza pública. En el caso concreto, el Grupo Parlamentario reconoció la comunicación y sostuvo que el hecho de que los datos no estuvieran disociados se debió a un error.

La Agencia estimó que el tratamiento de datos necesario para ilustrar y respaldar una información de indudable relevancia pública como es la relativa a un caso de corrupción que se quería difundir no justifica que se divulguen datos especialmente protegidos referentes a la militancia de terceras personas sin relevancia pública, que no aportan información alguna de interés para el supuesto y que suponen una divulgación y tratamiento inadecuado, no pertinente y excesivo. En consecuencia, considera que se realizó un tratamiento de datos de carácter personal que revelan ideología consistente en su cesión o comunicación a terceros sin el consentimiento de los afectados y sin que concurra otra causa de justificación y concluye declarando que se ha producido una vulneración del art. 7.2 de la LOPD, calificada como muy grave en su artículo 44.4.b).

- **Notificación y emplazamiento para personarse en un recurso a través de una página web - AP/00039/2014**

Los participantes en un proceso selectivo para ingresar como vigilantes de sala de un museo, frente al que han planteado un recurso contencioso administrativo, denuncian que este ha publicado en su página web una resolución con sus datos personales. En la resolución, dictada a requerimiento judicial, se notifica a todos los interesados (un total de 18.514) la interposición del recurso y se les emplaza para que puedan personarse como demandados. El artículo 55.6 de la Ley 30/1992, de 26 de noviembre, establece que la convocatoria de un proceso selectivo indicará los medios de comunicación a través de los que llevar a cabo la sucesivas notificaciones, que en este caso fue la página web del museo. La notificación de la resolución, al adecuarse a la forma prevista en la convocatoria, no supone infracción de la normativa de protección de datos por lo que se archivó el procedimiento.

- **Tratamiento de datos con motivo de un proceso electoral en una corporación de derecho público - E/01194/2014, E/01515/2014, E/1516/2014 y E/01517/2014**

Se denuncia a una asociación y a una candidatura electoral en una corporación de derecho público por el tratamiento de datos personales sin consentimiento de los afectados realizado durante la jornada electoral para elegir a la Junta de Gobierno y al decano de un Colegio de Abogados. En concreto, por utilizar los datos de los electores que votaban para cruzarlos con el censo de electores y llamar a quienes no lo hubieran hecho. Como se señaló en la sentencia sobre el proceso electoral recaída en vía contencioso administrativa, existe un interés legítimo en captar el voto incluso durante la jornada electoral. Los datos tratados proceden en su mayor parte del listado de colegiados, una fuente de acceso público. Además, la participación como candidatos en un proceso electoral permite el tratamiento de los datos por concurrir un interés legítimo compatible con los derechos y libertades de los interesados. En cuanto a la cesión a terceros no se ha tenido acceso a conocer el alcance de los datos, su procedencia, ni el contenido de las llamadas efectuadas a los colegiados que no habían votado. Se archivaron las denuncias.

2

PROCEDIMIENTOS DE TUTELA DE DERECHOS

En términos generales, las reclamaciones de tutela de derechos han crecido en 2014 un 5,11% respecto a 2013, ascendiendo a 2.099[2]. Destacan un año más las solicitudes del derecho de cancelación (1.196), ocupando el segundo lugar las relativas al ejercicio del derecho de acceso (626). Las tutelas sobre los derechos de oposición y rectificación han ascendido a 147 y 95 respectivamente.

Como se ha mencionado en memorias anteriores, los ciudadanos en España han sido pioneros en ejercitar el denominado derecho al olvido (derechos de cancelación y oposición) para evitar la difusión universal, permanente e indiscriminada de sus datos personales en internet. En este sentido, debe subrayarse la indudable trascendencia de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 que reconoce, como ya venía aplicando la Agencia en sus resoluciones, que los buscadores de internet realizan un tratamiento de datos del que son responsables y que las personas tienen derecho a solicitarles, con las condiciones establecidas en la Directiva de protección de datos, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre. La sentencia se comenta con detalle en otro apartado de la Memoria. Los efectos de esta sentencia también se han hecho notar en el número de reclamaciones presentadas ante la Agencia. Así, de las 210 presentadas frente a buscadores en 2014, el 83,33% de ellas (175) fueron presentadas con posterioridad al 1 de junio de 2014.

[2] Esta cifra no coincide con el número de tutelas presentadas ya que hay reclamaciones que solicitan la tutela de más de un derecho.

A continuación se relacionan algunos de los procedimientos de tutela de derechos más destacados tramitados en 2014:

- **Acceso al informe pericial médico - TD/01492/2013**

No procede el acceso al informe pericial que determina las valoraciones o apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas por el afectado en un baremo para la cuantificación de la indemnización a percibir, pues no deben considerarse como «datos base» a los efectos del artículo 29 del RLOPD.

- **Acceso a la documentación bancaria del cónyuge en régimen de gananciales - TD/02014/2013**

El derecho de acceso es el derecho del interesado a obtener información de sus datos personales, pero no ampara el acceso a documentos concretos. El acceso a información como la relativa a los productos bancarios suscritos a su nombre o de su ex marido queda fuera del ámbito competencial de la Agencia, que se limita a determinar si se han cumplido los requisitos legales y reglamentarios establecidos para el tratamiento de los datos sin realizar indagaciones propias de la esfera civil, que deben instarse ante los órganos administrativos o judiciales competentes.

- **Acceso y rectificación del historial clínico - TD/00158/2014**

El reclamante ejercitó el derecho de acceso a su historia clínica ante la entidad reclamada y la misma resolvió la solicitud conforme con lo establecido en la normativa de protección de datos, proporcionando al reclamante el informe médico requerido. No puede pretenderse a través de la Agencia Española de Protección de Datos la rectificación o can-

celación del contenido de un informe médico ni de las valoraciones y conclusiones recogidas en el mismo, que ha sido elaborado por un facultativo en el ejercicio de su profesión. En el mismo sentido que este procedimiento se resolvió la TD/00672/2014 sobre una solicitud que requería rectificar el contenido, valoraciones y conclusiones recogidas en un informe pericial elaborado por un psicólogo en el ejercicio de su profesión.

- **Cancelación en la historia clínica - TD/01051/2014**

Se rechazó la solicitud de rectificación y cancelación frente a un servicio de salud por considerar que los datos contenidos en la historia clínica (HC) del reclamante no eran inadecuados, incompletos ni inexactos. Procede la denegación porque el contenido de las HC debe ser conservado durante el plazo que establece la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y, en este caso, se ha solicitado antes de que dicho plazo haya transcurrido.

- **Acceso a huellas dactilares en un fichero policial - TD/00024/2014**

El reclamante ejercitó su derecho de acceso ante la Dirección General de la Policía (DGP) y esta le informó de que en uno de sus ficheros figuraba inscrita la reseña decadactilar (impresiones dactilares de los diez dedos). Examinada la documentación aportada por ambas partes, se observa que la DGP contestó al reclamante al derecho de acceso y a la posterior ampliación de dicho derecho, informándole de que sólo figuraba inscrita la reseña decadactilar. Sin embargo, no consta que esas impresiones dactilares, que son datos personales, le hayan sido facilitadas, procediéndose a estimar la reclamación.

- **Prevalencia de los procedimientos especiales de cancelación - TD/00441/2014**

Un ciudadano ejercitó su derecho de cancelación en relación con un expediente por la negativa de la delegación de una prelatura religiosa a notificarle por escrito el rescripto de dispensa que el prelado emite al rescindir un miembro de la misma el acuerdo-contrato que le vincula a la prelatura personal.

El artículo 25.8 del Reglamento de la LOPD dispone que «cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas». Por tanto, el contenido de la solicitud planteada por el reclamante hubiera debido resolverse de conformidad con la normativa especial aplicable, no correspondiendo a esta Agencia interpretar las previsiones sobre el cambio de residencia de un fiel diocesano así como otras cuestiones similares planteadas.

TD/01496/2014 - Se solicitó la cancelación de datos incluidos en un fichero de la Dirección General de Tráfico, relacionados con la comisión de infracciones de tráfico. En aplicación del art. 25.8 RLOPD se desestimó la tutela al existir un procedimiento específico en la normativa de seguridad vial.

- **Cancelación de los datos penitenciarios por una sentencia absolutoria - TD/00803/2014**

Se solicita la tutela frente a la Dirección General de Instituciones Penitenciarias (DGIP) para que proceda a cancelar los datos del reclamante como preso preventivo al haber sido absuelto. La DGIP contestó al reclamante exigiéndole la presentación de certificación negativa de antecedentes penales e informándole de que la Comisión Calificadora de Documentos Administrativos del Ministerio del In-

terior dictaminó que los expedientes personales de los internos eran de conservación permanente. La DGIP manifiesta que, tras haber recibido la resolución de firmeza de la sentencia absolutoria, ha procedido a cancelar sus datos.

- **Improcedencia del derecho de cancelación de datos profesionales - TD/01011/2014**

Se presentó una reclamación frente a la respuesta recibida tras haber ejercitado el derecho de cancelación ante una empresa suministradora de información mercantil y comercial que se lo había denegado al reclamante. Los datos cuya cancelación solicita son de carácter eminentemente profesional, pues se refieren el nombre y apellidos de los órganos sociales nombrados por empresas, y proceden del Boletín del Registro Mercantil. El reclamante no ha invocado ni probado su obsolescencia por lo que, de conformidad con lo dispuesto en el artículo 2.2 del RLOPD, quedan excluidos del ámbito de la normativa de protección de datos. En consecuencia, y dado que la entidad respondió al reclamante, se inadmitió la reclamación. Sin embargo, en las **TD/00867/2014** y **TD/00888/2014** se analizó el tratamiento de la dirección y domicilio particular del reclamante que aparecen asociados a una empresa y, aunque la entidad alegó que son datos del representante de una persona jurídica, este hecho no fue acreditado, no coincidiendo con la dirección que obraba en el Registro Mercantil. En consecuencia, se estimaron las reclamaciones y se instó a la entidad para que remitiera certificación de haber atendido el derecho de cancelación.

- **Derecho de oposición a recibir información sindical a través del correo electrónico corporativo - TD/00869/2014**

Se solicitó la tutela del derecho de oposición frente a un sindicato para que dieran de baja al reclamante en los envíos de comunicaciones sindicales que realizan a su correo corporativo. Aunque la remisión de información por los sindicatos a los trabajadores está amparada por el derecho a la libertad sindical y no se necesita el consentimiento del interesado, éste puede ejercer el derecho de oposición salvo en periodo previo a las elecciones sindicales. En el presente caso, el reclamante se dirigió al sindicato para que no le enviara más información sindical. Este último alegó que no era el responsable del fichero pero el uso de la dirección de correo electrónico para el envío de la información implica un tratamiento de datos del que es responsable y, como tal, debe garantizar el ejercicio de los derechos ARCO. En consecuencia, se estimó la tutela y se requirió a la entidad para que remitiera al reclamante certificación de haber atendido su derecho.

- **Ejercicio abusivo del derecho de acceso - TD/01938/2014 y TD/01312/2014**

El reclamante presentó 16 reclamaciones de tutela de derechos en su nombre y otras 14 en nombre de su hija menor de edad frente a ficheros de distintos responsables de las Administraciones Públicas. De los antecedentes obrantes en la Agencia, en los que consta la presentación con anterioridad de numerosas reclamaciones tanto del propio reclamante como en representación de su hija (más de 200), se desprende la concurrencia de los requisitos para calificarlas de abuso de derecho señalado por la jurisprudencia al cuestionarse la ausencia de finalidad seria y legítima y existir un objetivo exceso en el ejercicio del derecho. En consecuencia, la inexistencia de legítimo interés determinó la inadmisión de las reclamaciones.

Respecto del tratamiento de datos personales en internet cabe destacar las siguientes resoluciones:

- **Contenido en red social - TD/00688/2014**

Se reclamaba la supresión de un vídeo grabado al reclamante sin su consentimiento y publicado en

<Índice>

una red social en el que aparecía realizando sus tareas de vigilante de seguridad y sobre el que se vertían insultos y amenazas. Se solicitó la tutela del derecho de cancelación basándose en que la difusión del vídeo estaba sometiendo al reclamante a una gran presión psicológica que amenazaba su vida personal y laboral, y manifestando que el responsable de la publicación y difusión del vídeo había sido condenado por una falta de injurias, pero que no había retirado el vídeo de su perfil.

Ningún ciudadano que no sea un personaje público ni sea objeto de un hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal resulten accesibles en la Red sin poder reaccionar ni corregir la inclusión ilegítima de los mismos.

La solicitud de tutela se estimó para evitar que la difusión de los datos del reclamante tuviera efectos no deseados con carácter permanente. Aunque la red social no es responsable de los contenidos ofrecidos por los usuarios, debe realizar las gestiones necesarias para su retirada cuando la AEPD, como órgano competente, lo requiera.

- **Contenidos en Boletines Oficiales**

En el procedimiento **TD/01544/2013** el reclamante ejercitó su derecho de oposición porque sus datos personales aparecían publicados en un boletín del año 2008 en una resolución por la que se publicaba la relación de aspirantes a ingreso en el Cuerpo Nacional de Policía que aprobaron la fase de oposición y se nombraban policías alumnos.

Dicha publicación se exige por la normativa específica reguladora del Cuerpo Nacional de Policía que, entre otras cuestiones, establece las condiciones y requisitos que han de cumplir los aspirantes, siendo requisito indispensable la publicación en el BOE de su nombramiento para la adquisición de la condición de funcionario de carrera del citado Cuerpo.

Cuestión distinta es el derecho del ciudadano a oponerse —en el caso de que exista un motivo legítimo y fundado en el sentido previsto en la ley— a que sus datos personales sean objeto de tratamiento, inhabilitando su posible captación por los buscadores de internet cuando se realiza una búsqueda a partir de su nombre. En el presente caso, a pesar de la normativa anteriormente indicada, que exige la publicación del nombramiento, hay que tener en cuenta las implicaciones en materia de seguridad que pueden derivar de la divulgación masiva de su pertenencia a las Fuerzas y Cuerpos de Seguridad del Estado, procediendo estimar la pretensión del reclamante.

El BOE, al utilizar como medio de publicación la edición electrónica, está obligado a adoptar las medidas necesarias y adecuadas según el estado actual de la tecnología para evitar la indexación de los datos personales del reclamante en sus páginas con objeto de que en el futuro los motores de búsqueda de internet no puedan asociarlas al reclamante y con ello se impida la divulgación de manera indiscriminada de sus datos personales.

En sentido similar se dictó la resolución **TD/01133/2014** frente al tratamiento en la página web del BOE de los datos del reclamante, recogidos en una resolución de la Secretaría de Estado de Seguridad de 2005 que contenía la relación de participantes declarados aptos para las pruebas de selección de vigilantes de seguridad y sus especialidades. El BOE denegó la solicitud del reclamante alegando que se trataba de una resolución publicada conforme a la normativa vigente por cuya autenticidad e integridad debía velar. No obstante, las publicaciones del BOE están sometidas al ordenamiento jurídico en su conjunto y, por tanto,

también a la LOPD cuando incluyan datos personales. El reclamante no puede oponerse al mantenimiento de sus datos en el BOE al estar la publicación legitimada por la ley, pero sí puede oponerse a su posible captación por los buscadores de internet si existe un motivo legítimo, como en el presente caso, que se justifica tanto por el tiempo transcurrido como por la relación de la información con la seguridad, que puede ocasionar graves repercusiones para el reclamante.

Por el contrario, en la **TD/01063/2014** se solicitó la tutela del derecho de oposición frente al BOE porque el reclamante consideró insuficiente la respuesta de que se iban a incorporar las referencias correspondientes en el robots.txt. La Agencia estimó que el responsable del tratamiento había actuado correctamente al entender que la utilización de la herramienta robots.txt es un método válido para evitar la indexación de la información por parte de los buscadores, evitando la difusión indiscriminada de la información. Un caso similar es el de la resolución **TD/01708/2013,** en cuyo procedimiento se constató que una diputación provincial había puesto los medios necesarios para impedir que buscadores indexaran las ediciones electrónicas del boletín, que sólo se podían consultar en su propia Sede electrónica. Por ello, es el buscador, en su caso, el que debe actualizar sus índices de búsqueda para evitar una posible indexación.

- **Derecho de oposición frente al BOE y a un buscador. Información no obsoleta - TD/00711/2014**

Se solicitó la tutela del derecho de oposición frente al BOE y a un buscador para desindexar –cuando se buscaban por el nombre y los apellidos– los enlaces web de la publicación en 2012 en el BOE del Real Decreto de indulto del reclamante. El buscador esgrime que no le es de aplicación la normativa europea, al prestar sus servicios desde EEUU. Frente a estas alegaciones, y como recoge la sentencia del TJUE de 13 de mayo de 2014, el gestor del motor de búsqueda es responsable del tratamiento de los datos al determinar los fines y los medios de la actividad que desarrolla, resultando plenamente aplicable la legislación nacional para resolver una solicitud de tutela, que se puede instar directamente frente al buscador de internet sin acudir necesariamente al responsable del sitio web. El BOE debe adecuar su actuación a lo señalado en la síntesis de la resolución anterior. En cuanto a la procedencia de la tutela solicitada se concluyó que había de ser rechazada por cuanto se trataba de una información que no era obsoleta, ya que el indulto estaba condicionado a que no se abandonara el tratamiento iniciado por el reclamante y a que no delinquiera en un plazo de tres años desde su publicación. Por tanto, se inadmitió la reclamación.

En sentido contrario, se estimó la reclamación de un ciudadano frente al BOE **(TD/00885/2014)** referida a un indulto de 1996, y la **TD/01358/2014** referida a un indulto de 1972 frente al buscador al haber transcurrido el plazo establecido para no reincidir en la comisión de delitos.

- **Hechos de relevancia pública. Improcedencia del derecho de cancelación - TD/01168/2014**

Se solicitó la tutela del derecho de cancelación frente a un medio de comunicación y frente a un buscador para que procedieran a cancelar el acceso a una información referente a la participación de los reclamantes en un negocio piramidal con numerosas personas afectadas. Los conflictos entre la libertad de información y expresión y el derecho a la protección de datos han sido resueltos por el Tribunal Constitucional en favor de la prevalencia de aquél siempre que los hechos publicados se

<Índice>

consideren de relevancia pública. En el presente caso, la información publicada no ha quedado obsoleta ni se ha demostrado inexacta, pues la sentencia aportada por los reclamantes no prejuzga su exactitud al circunscribirse a la correcta o incorrecta satisfacción del derecho de rectificación. En consideración a la trascendencia en el número de personas afectadas, el limitado tiempo transcurrido desde los hechos descritos y la publicación de la noticia así como la relevancia pública que alcanzó la reclamante, se desestimó la tutela tanto frente al medio como frente al buscador.

- **Derecho de cancelación frente a un buscador. Información relevante y no obsoleta - TD/01363/2014**

Se solicitó la tutela del derecho de cancelación frente a un buscador para que desindexara una página web en la que se recogía una noticia referente al reclamante en la que se le acusaba de realizar inversiones en el extranjero, participando en un conocido caso de corrupción organizada. En este caso la información resultaba de interés para la opinión pública, no siendo incierta ni obsoleta, por lo que su tratamiento estaba legitimado y no vulneraba la normativa de protección de datos. Se inadmitió la tutela.

Por el contrario, han sido varias las reclamaciones estimatorias referentes a tratamientos de datos inexactos o inicialmente lícitos pero que, dado el tiempo transcurrido, actualmente son excesivos y no resultan pertinentes para los fines que motivaron su tratamiento. Así, la **TD/00066/2014** se refirió a la publicación de un edicto de notificación a deudores fechado en octubre de 2012. También se estimó la reclamación planteada en la **TD/01997/2013** al objeto de que se evitara el acceso a los datos personales del reclamante que aparecían en dos enlaces web, uno del Congreso de los Diputados y otro de la hemeroteca de un diario, referentes a una información sobre la comisión de un homicidio doloso que se publicó en el Boletín Oficial del Congreso de los Diputados hace más de veinte años.

A pesar de que el tratamiento de los datos en el enlace reclamado fue inicialmente lícito, posteriormente esos datos pueden considerarse no pertinentes o excesivos desde el punto de vista de los fines para los que fueron tratados por el tiempo que ha transcurrido y al haberse cumplido la función de la notificación de dicha publicación.

Consecuentemente, se resolvió estimando la exclusión de los datos personales respecto del citado enlace al tratarse de datos obsoletos y no concurrir «un interés preponderante del público a acceder a la información a través de una búsqueda en internet que verse sobre el nombre de la persona».

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 en 2014 fueron informadas 157 disposiciones de carácter general, lo que supone un máximo en el número de disposiciones sujetas a informe, con un incremento del 13% respecto del ejercicio anterior y un aumento acumulado del 64% en relación con las cifras de 2012. Dicho incremento se debe en parte, como en 2013, a la emisión de 32 informes a disposiciones provenientes de la Comunidad de Madrid como consecuen-

2

cia de la supresión de su Agencia autonómica de protección de datos.

De entre las disposiciones sometidas al parecer de la Agencia cabe hacer referencia a las siguientes:

- Anteproyecto de Ley Orgánica del Poder Judicial.
- Anteproyecto de Ley Orgánica complementaria de la Ley de Protección a la Infancia.
- Anteproyecto de Ley Orgánica para la protección de la vida del concebido y de los derechos de la mujer embarazada.
- Anteproyecto de Ley por la que se regula el estatuto del miembro nacional de Eurojust y las relaciones con este órgano de la Unión Europea, las redes judiciales de cooperación internacional y los magistrados de enlace.
- Anteproyecto de Ley de Protección a la Infancia.
- Anteproyecto de Ley de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- Anteproyecto de Ley de modificación parcial de la Ley 58/2003, de 17 de diciembre, General Tributaria.

<Índice>

- Anteproyecto de Ley de medidas en materia de liquidación e ingreso de cuotas de la Seguridad Social.

- Anteproyecto de Ley por el que se establece la normativa básica del comercio y tenencia responsable de perros y gatos.

- Proyecto de Real Decreto por el que se aprueba el reglamento de desarrollo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

- Proyecto de Real Decreto por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo.

- Proyecto de Real Decreto por el que se aprueba el Reglamento de la Comisión de Vigilancia de actividades de financiación del terrorismo.

- Proyecto de Real Decreto por el que se modifica el Reglamento General de Circulación.

- Proyecto de Real Decreto por el que se aprueba el Reglamento sobre la adquisición de la nacionalidad española por residencia.

- Proyecto de Real Decreto por el que se regula el Registro de Entidades Religiosas.

- Proyecto de Real Decreto por el que se aprueba el reglamento del Registro Mercantil.

- Proyecto de Real Decreto por el que se establecen las normas complementarias al reglamento hipotecario en materia de registro electrónico.

- Proyecto de Real Decreto por el que se aprueba el Reglamento del Registro Nacional de Asociaciones.

- Proyecto de Real Decreto de estructura y contenidos básicos del Registro de Actividad de Atención Especializada.

- Proyecto de Real Decreto por el que se regulan las especificaciones y condiciones para el empleo del Documento Único Electrónico (DUE) para la puesta en marcha de sociedades cooperativas, sociedades civiles, comunidades de bienes, sociedades limitadas laborales y emprendedores de responsabilidad limitada mediante el sistema de tramitación telemática.

- Proyecto de Real Decreto por el que se regulan las especificaciones y condiciones para el empleo del Documento Único Electrónico (DUE) para la extinción y el cese de la actividad de las empresas.

- 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 crea el fichero de datos de carácter personal cl@ve del Ministerio de la Presidencia.

- Proyecto de Orden sobre difusión y publicidad de las resoluciones concursales a través de Internet.

- Proyecto de Orden por la que se dictan las disposiciones necesarias para la puesta en funcionamiento del Registro de Mediadores e Instituciones de Mediación.

- Proyecto de Orden por la que se modifica la Orden por la que se crea el de Receta Electrónica en el Sistema Nacional de Salud.

- Proyecto de Orden por la que se modifica la Orden SPI/2136/2011, de 19 de julio, por la

que se fijan las modalidades de control sanitario en frontera por la inspección farmacéutica y se regula el Sistema Informático de Inspección Farmacéutica de Sanidad Exterior.

- Proyecto de Orden por la que se concreta y actualiza la cartera común básica de servicios asistenciales del Sistema Nacional de Salud y se regulan los estudios de monitorización de técnicas, tecnologías y procedimientos.

- Proyecto de Orden por la que se regula la comunicación de la información relativa a los accidentes de tráfico y las víctimas al Registro Estatal de Víctimas de Accidentes de Tráfico.

- Proyecto de Orden de creación del fichero de datos de carácter personal «Fichero de Titularidades Financieras» del Ministerio de Economía y Competitividad.

- Proyecto de Instrucción de la Secretaría de Estado de Economía y Apoyo a la Empresa, por la que se establecen los datos de identificación adicionales que deben ser declarados por las entidades de crédito al Fichero de Titularidades Financieras a fin de la adecuada identificación de intervinientes, cuentas y depósitos.

- Proyecto de Acuerdo del Pleno del Consejo General del Notariado de creación del fichero de titularidad pública denominado «base de datos de personas de responsabilidad pública».

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 2014 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 236 sentencias, de las cuales:

- 164 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (70%).

- 23 estimaron parcialmente los recursos (10%).

- 34 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (14%).

- 15 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (6%).

Debe tenerse en cuenta que se ha producido el desistimiento por parte del demandante en 136 recursos, confirmándose así la resolución de la Agencia objeto del recurso. Se trata de un gran número de los recursos interpuestos por Google contra resoluciones de la Agencia que estimaban la solicitud de cancelación u oposición planteada por el interesado y que se veían afectados por lo señalado en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, a la que se hace referencia en otro lugar de esta Memoria. Del mismo modo, debe indicarse que como consecuencia de la aplicación de dicha sentencia se han dictado en este ejercicio 35 sentencias, siendo 24 desestimatorias, 10 estimatorias y una parcialmente estimatoria, por lo que el efecto de esas resoluciones judiciales sobre las cifras totales no se ve afectado.

A la vista de las cifras generales que se han mencionado, cabe concluir que la confirmación de los criterios de la Agencia en cuanto al fondo del asunto ha sido de un 76%, incrementándose así en cuatro puntos porcentuales sobre las del año 2013, alcanzándose así la mejor cifra de sentencias favorables desde el año 2006. Además, el porcentaje de sentencias en que se estiman íntegramente las pretensiones del recurrente es el más bajo desde el año 2005.

<Índice>

Al propio tiempo, se observa un notable descenso de la litigiosidad referida a la actuación de la Agencia, por cuanto el número total de sentencias se reduce en casi un 16%.

En relación con los sectores de actividad a los que afectan las sentencias dictadas el sector que presenta una mayor litigiosidad sigue siendo el de las telecomunicaciones, con un 27% del total, si bien se reduce en gran medida el porcentaje que representan las sentencias del sector en 16 puntos porcentuales, siendo además del 46% su disminución en términos absolutos. Asimismo, cabe hacer referencia al sector financiero (con un 14% del total), a los recursos interpuestos por los particulares, bien contra resoluciones de archivo de actuaciones, bien contra resoluciones desestimatorias en procedimientos de tutela de derechos —que mantiene cifras ligeramente inferiores a las de 2013 (11% del total)— y a los recursos interpuestos por empresas del sector energético y gasista (un 10%).

Es muy significativo el incremento de las sentencias relacionadas con empresas de servicios de asesoría y consultoría (13 frente a una única sentencia en 2013), si bien 11 de las 13 sentencias de este sector se refieren a una sola empresa y se relacionan con la prestación de servicios para la contratación con una empresa del sector energético. Igualmente, debe reiterarse lo ya señalado en la Memoria de 2013 en relación con el incremento de los recursos interpuestos por empresas del sector energético: si en el año 2012 su volumen era de un 3% del total, incrementándose al 8% en 2013, ya ha quedado dicho que en el año 2014 representan un 10%, siendo uno de los pocos sectores en los que aumenta el número de sentencias respecto del ejercicio anterior, pese a la disminución total del número de sentencias en un 16%. Igualmente aumentan en términos absolutos las sentencias relacionadas con el sector de la publicidad y prospección comercial.

Mención aparte debe efectuarse a los recursos interpuestos por empresas prestadoras de servicios de la sociedad de la información, que se han incrementado desde una única resolución judicial en 2013 a 38 en 2014. No obstante, este incremento se debe a las 35 sentencias que resuelven recursos interpuestos por Google, por lo que puede considerarse que esta circunstancia implica una sensible desviación en lo que afecta al peso de este sector.

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 de la normativa de protección de datos, las SSAN 15/4/14, 30/4/14 y 10/7/14 consideran que la expresión «cobro de morosos» contenida en un sobre en que aparecen los datos identificativos de una persona implica la revelación del dato personal «moroso». Por su parte, la SAN 19/3/14 considera la voz como un dato personal, siendo igualmente numerosas las sentencias que consideran dato personal las imágenes captadas por dispositivos de videovigilancia.

- En cuanto a la aplicabilidad de las normas de protección de datos, la SAN 20/6/14 considera que es un tratamiento para fines exclusivamente personales o domésticos el realizado por un

arrendador persona física respecto de la correspondencia que le haya remitido el arrendatario. Por su parte, varias sentencias se refieren a la exclusión de la normativa a los empresarios individuales. Así, las SSAN 12/6/14 y 20/6/14 consideran que una persona física no pierde esta condición y se considera empresario individual por el solo hecho de aparecer en un directorio comercial como las páginas amarillas y la SAN 21/11/14 entiende que tampoco desaparece esta condición por la firma de un contrato de telefonía para empresas o autónomos. En todo caso, la SAN 28/10/24 recuerda que deberá estarse en cada caso a la finalidad del tratamiento y la naturaleza de los datos. Finalmente, en relación con la aplicación de esta norma, la SAN 19/3/14 considera que los datos referidos a las adquisiciones de medicamentos efectuadas por una oficina de farmacia no son datos personales.

- En relación con las competencias de la AEPD, las SSAN 13/5/14 y 21/7/14 confirman que la misma no las ostenta en relación con los ficheros judiciales, no pudiendo enjuiciar la validez de una cesión de testimonio de unos autos acordada por un Juzgado ni para conocer la reclamación planteada por la cesión por Juzgados y Tribunales a un Colegio de Procuradores de datos para el cálculo de la cuota variable.

- Por lo que respecta al deber de información, la SAN 19/2/14 recuerda que la anulación del artículo 18 RLOPD por la STS de 15/7/10 no exonera de la carga de la prueba por el responsable del cumplimiento del deber de informar, pues ese precepto solamente se refería a la forma de conservación de esa prueba.

- La AN por su parte, ha mantenido en distintas sentencias la aplicación del artículo 7.f) de la Directiva 95/46/CE. Particularmente puede hacerse mención de las que se han referido a la prevalencia de la libertad sindical en su acepción de libertad de información sindical (SAN 12/6/14, referida a la publicación en la web de un sindicato de una sentencia condenatoria del secretario general de otro sindicato por entorpecer el ejercicio de la libertad sindical) o, si se dan los requisitos de proporcionalidad legalmente exigibles, en el ámbito de la videovigilancia (doctrina posteriormente convalidada por el TJUE). Por el contrario, se ha considerado insuficiente para la aplicación del artículo 7.f) el interés meramente comercial del responsable (SAN 23/2/14). Del mismo modo, se considera que no es posible ampararse en esta previsión para publicar en un sitio web una información cuya falta de veracidad había sido expresamente acreditada (SAN 24/10/14).

- Son diversos los supuestos en que la AN ha confirmado el criterio de la AEPD en el sentido de considerar que no existía legitimación suficiente para el tratamiento. Así, puede hacerse referencia a los supuestos de inclusión en una guía telefónica de datos que no figuran en el fichero facilitado por la CMT (SAN 28/10/14) o en la inclusión de los datos del interesado sin haberle informado de la posibilidad de no aparecer en las guías (SAN 21/11/14). Tampoco existe legitimación para la realización de envíos publicitarios a quien expresamente había solicitado dar por concluida cualquier relación con el responsable y la cancelación de todos sus datos (SAN 1/4/14) o en los supuestos de cesión de créditos que ya habían sido satisfechos (SAN 21/10/14) o condonados (SAN 16/2/14).

- Como en otros ejercicios, son muy numerosas las sentencias relacionadas con el tratamiento de datos personales asociados a la contratación de servicios como el telefónico o el

<Índice>

eléctrico. Como primera consideración, las SSAN 5/3/14 y SAN 26/3/14 recuerdan que la prueba de la contratación corresponde al responsable, dado que exigir al denunciante la prueba de la no celebración del contrato constituiría una *probatio diabollica.* Del mismo modo, recuerda la SAN 7/2/2014 que la vulneración de la LOPD en cada caso constituye una infracción distinta, no cabiendo acumular como una infracción varios de estos casos. Además, la SAN 7/2/2014 considera que el pago de los recibos eléctricos no enerva la inexistencia, dado que se trata de evitar el corte en el suministro.

- Por su parte, la SAN 24/10/14 aprecia que existe consentimiento a la contratación en caso de verificación a través de un tercero de la contratación de telefonía. Asimismo, la SAN 30/10/14 estimó la existencia de indicios suficientes al existir en el contrato con firma similar a la contenida en la denuncia y haberse llevado a cabo una prueba pericial caligráfica de la que se deducen indicios en este sentido. Por su parte, la SAN 7/3/14, aunque considerando probado que se ha dado una suplantación, exonera de culpa al responsable al constar en su documentación un DNI en que el nombre y número coinciden con el del denunciante pero se habían modificado los demás datos al haber sido falsificado.

- Por el contrario, se aprecia la inexistencia de indicios suficientes en los casos en que no se aporta la grabación de un contrato que se afirma celebrado telefónicamente (SAN 10/7/14), los supuestos en que se emitieron facturas después de que se hubiera resuelto por el responsable el contrato al apreciarse indicios de fraude (SAN 17/6/14) o después de que se remitiese por el afectado un burofax solicitando la baja. Tampoco hay indicios en los casos en que no consta el DNI del denunciante y su firma difiere de la que consta en el expediente (SAN 21/11/14) o en que se utiliza el NIE de una persona que actualmente tiene nacionalidad española para la contratación de un servicio, sin que conste su firma en el contrato (SAN 11/11/14). También se considera que hay indicios de vulneración en los casos de uso de datos de un cliente para la facturación del consumo telefónico de una línea distinta (SAN 22/1/14), o de uso de datos de un cliente del servicio de gas para facturarle el suministro eléctrico (SAN 7/2/14), así como en los casos de falta de la preceptiva verificación en contratación telefónica (SAN 12/3/14).

- En relación con los datos de salud, la SAN 5/5/14 confirma la infracción de la LOPD como consecuencia de la alteración automática por un servicio de salud de las prescripciones médicas de los pacientes, reemplazando el medicamento de marca por el genérico, considerando que hay un tratamiento de datos de salud. La SAN 10/7/14 confirma el incumplimiento de la LOPD, en conexión con la Ley de autonomía del paciente, por haberse producido la destrucción de datos de historias clínicas antes de haber transcurrido cinco años.

- Respecto del derecho de acceso, la Audiencia ha confirmado que el mismo no comprende el derecho a conocer los usuarios que han accedido a los datos (SAN 26/2/14) ni el acceso a documentos (SAN 16/9/14). Del mismo modo, se ha confirmado la denegación del derecho en los casos en que se solicita al prestador de servicios de comunicaciones electrónicas información de quiénes han accedido a una cuenta de correo electrónico asignada por aquél al afectado (SAN 12/2/2014) o se solicita información de las comunicaciones electrónicas efectuadas entre el domicilio del reclamante y un servidor

determinado (SAN 30/9/14). Tampoco procede cuando se solicita el acceso a una grabación de una llamada al 112 en que se escucha no sólo la voz del solicitante sino de terceras personas (SAN 19/3/14).

■ En materia de seguridad, la SAN 15/7/14 ha considerado vulnerado este principio al producirse un error de configuración en la página web de una aseguradora, que permitió acceder a través de buscadores a datos de salud de su servicio de reclamaciones. Igualmente, se ha declarado la existencia de infracción del deber de seguridad en los casos de remisión de sobres con los datos identificativos de un afectado y la leyenda «cobro de morosos».

■ Se ha declarado, por otra parte, la vulneración del deber de secreto en el caso de envío de una factura telefónica desglosada a la expareja del abonado (SAN 15/7/14) o por el envío de un correo electrónico por error a persona distinta de su destinataria, incluyendo datos personales incorporados a correos previos entre la denunciante y la responsable (SAN 26/6/14).

■ En el ámbito de los ficheros de solvencia, la Audiencia ha considerado que no existe certeza de la deuda cuando existe una reclamación a una junta arbitral de consumo (SSAN 2/7/14 y 21/11/14) o en el caso de que exista una demanda judicial reclamando la nulidad del contrato del que trae causa la deuda, notificada por burofax al acreedor antes de la inclusión de los datos en el fichero (SAN 20/6/14). También se ha considerado que no era lícita la inclusión de una deuda derivada del envío de tarjeta de crédito y el PIN de activación de la misma a una dirección errónea (SAN 24/4/14).

■ En relación con el cumplimiento por parte del acreedor de la obligación de requerimiento de pago previo a la inclusión de los datos en el fichero de solvencia, la SAN 19/2/14 considera que la misma podría acreditarse a través de la prueba permitida al responsable del fichero común en el RLOPD, y la SAN 1/7/14 recuerda que dicha notificación no subsanará la falta de requerimiento. Igualmente, las SSAN 12/6/14, 20/6/14 y 17/10/14 consideran insuficiente la mera aportación del protocolo seguido por el acreedor en estos casos sin aportarse prueba suficiente de su realización. Del mismo modo, se señala que no basta la mera certificación de la entrega del requerimiento en correos (SAN 1/7/14) ni el albarán de entrega y la facturación de servicios por la empresa encargada de dicha entrega (SAN 3/4/14). Tampoco se ha considerado válido el requerimiento efectuado por SMS, al no poder probarse su recepción (SAN 22/1/2014), o su remisión posterior a la inclusión (SSAN 24/1/2014 y 10/7/14).

■ Por otra parte, la Audiencia viene a reiterar la aplicación, prevista en el RLOPD de la regla que prohíbe el mantenimiento de la deuda en el fichero de solvencia una vez que la misma ha sido pagada (SAN 4/11/14) o ejecutada y embargados los bienes del deudor (SAN 15/4/14).

■ En el ámbito de la videovigilancia, las SSAN 22/1/2014 y 4/11/14 recuerdan el sometimiento a lo establecido en la LOPD y en la Instrucción 1/2006 de los supuestos de reproducción en tiempo real sin grabación de las imágenes. La SAN 22/1/2014 recuerda, por su parte, que el aviso informativo de la existencia de cámaras deberá asimilarse en lo esencial al contenido en dicha Instrucción. En cuanto a la existencia de proporcionalidad en el tratamiento debe hacerse referencia a dos sentencias, de 28/2/14 y 17/10/14 que exigen tener en cuenta el destino de las instalaciones en que se utilizan estos dis-

<Índice>

positivos, con independencia del uso que pudiera darse a las mismas por el personal (se trataba de cámaras situadas en lugares de paso que el personal utilizaba como vestuario, sin ser esa su función).

- También en este ámbito la SAN 15/7/14 considera proporcional la instalación de monitores en el interior de una entidad bancaria que reproducen las imágenes captadas en tiempo real, siendo las imágenes similares a las que se perciben sin las cámaras. Por el contrario, se ha negado la proporcionalidad en los casos de microcámaras situadas en cajeros automáticos que captan la vivienda situada enfrente de los mismos (SAN 15/7/14) o de grabación de soportales anejos a entidad financiera, incluyendo una terraza instalada en los mismos (SAN 22/11/14).

- En cuanto a la aplicación de las normas de la Ley 34/2002 referidas al envío de comunicaciones comerciales no solicitadas, la SAN 22/1/14 recuerda que no son de aplicación en estos casos las normas de protección de datos. Por otra parte, la SAN 24/6/14 exige atender, a fin de verificar si se ha prestado el consentimiento, al tenor real de la cláusula de consentimiento, y la SAN 7/10/14 considera que no cabe considerar servicios similares, a fin de eximir de la prestación del consentimiento la suscripción de un servicio para la obtención de contenidos exclusivos a través de telefonía móvil y el envío de comunicaciones relacionadas con la participación en un programa televisivo.

- En cuanto a las cuestiones relacionadas con la tramitación de los procedimientos de la Agencia, la Audiencia ha considerado que la misma puede no iniciar actuaciones si no aprecia que existen indicios de vulneración (SSAN 4/414 y 22/4/14); del mismo modo, es posible la apertura de un procedimiento sancionador si de la denuncia se infieren indicios suficientes para ello (SAN 4/11/14).

- En lo que respecta a la aplicación de los criterios de atenuación de la responsabilidad del artículo 45.5 de la LOPD, la AN ha considerado procedente la rebaja de la sanción en los siguientes casos: regularización rápida e indemnización al afectado (SAN 26/9/14), adopción de medidas correctoras de una quiebra de seguridad el mismo día en que se conoció su existencia (SAN 15/7/14), rectificación de la conducta infractora cuatro meses antes de la denuncia (SAN 10/7/14), recolocación de las cámaras y pixelado durante la tramitación del procedimiento en el caso de videovigilancia (SAN 8/4/14) o reestructuración societaria (SSAN 31/3/14 y 15/4/14).

- La AN, por último, ha recordado en sus sentencias de 24/4/14, 26/9/14 y 10/6/14 la naturaleza excepcional y no sancionadora del apercibimiento.

Por su parte, el **Tribunal Supremo** dictó un total de 9 resoluciones (7 sentencias y 2 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. Como ya se indicó en la Memoria correspondiente a 2013, el número de recursos ha sufrido una drástica reducción como consecuencia de la reforma operada en la Ley Jurisdiccional por la Ley 37/2011, de 10 de octubre.

En relación con estos recursos, el Tribunal Supremo:

- Declaró en cuatro 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 dos supuestos la inadmisión del recurso.

- Declaró en una ocasión no haber lugar al recurso interpuesto por la representación procesal de la Agencia contra una sentencia de la Audiencia Nacional que estimaba parcialmente el recurso interpuesto contra resolución de aquélla.

- Declaró en dos sentencias haber lugar a los recursos interpuestos contra sentencias que confirmaban las resoluciones de la Agencia.

De entre todas ellas cabe hacer especial referencia a la STS de 3/10/14, por la que se desestima el recurso de casación interpuesto contra sentencia de la Audiencia Nacional que confirmaba el criterio de la Agencia por una entidad gestora de derechos de autor que había solicitado la exención del deber de informar a los afectados de que llevaba a cabo un rastreo de redes P2P para la detección de las direcciones IP desde las que se ponen a disposición contenido protegidos por propiedad intelectual, considerando la Agencia que no procedía esa exención al no estar el tratamiento amparado en la LOPD. La sentencia, en primer lugar, declara que las direcciones IP tienen la condición de datos personales incluso aunque quien los trate no los asocie directamente *prima facie* con su titular. Además, confirma que el tratamiento carece de legitimación. En este sentido, considera que no es posible apreciar el consentimiento alegado por la entidad, dado que no puede considerarse prestado tácitamente si el interesado ni siquiera conoce que sus datos están siendo recogidos. Tampoco considera suficientemente clara y precisa la habilitación legal que se invocaba por la entidad, al amparo de las normas reguladoras de la propiedad intelectual y, finalmente considera que no procede la aplicación en este caso del artículo 7.f) de la Directiva 95/46, por cuanto el interés de la recurrente es meramente privado y no puede prevalecer sobre el derecho de los afectados, teniendo en particular en cuenta la especial trascendencia de los datos de tráfico en la vida privada del usuario.

Durante 2014 ha sido particularmente relevante la doctrina jurisprudencial emanada del **Tribunal de Justicia de la Unión Europea.** De este modo, y además de la sentencia de 13 de mayo de 2014, dictada en el asunto C 131/12 (Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González), que se detallará en el siguiente apartado de esta Memoria, cabe hacer referencia a otras tres sentencias:

- La sentencia de 8 de abril de 2014, recaída en los asuntos acumulados C-293/2012 y C-294/2012 (Digital Rights Ireland Ltd. y otros), cuya parte dispositiva declara inválida la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

  La sentencia establece en sus párrafos 32 a 37 que la medida prevista en la Directiva supone una injerencia en los derechos consagrados por los citados artículos 7 y 8 de la Carta, por lo que resulta necesario determinar si dicha injerencia resulta justificada en los términos que prevé la propia Carta, señalando que dicha injerencia respeta el contenido esencial de ambos derechos y que la medida de la que deriva la injerencia se fundamenta en un objetivo de interés general, haciendo referencia expresamente en su párrafo 44 la concurrencia de este requisito.

<Índice>

Sin embargo, a continuación, la sentencia se plantea si dicha injerencia resulta proporcionada al resultado perseguido, aplicando el triple juicio de idoneidad, necesidad y proporcionalidad en sentido estricto, poniendo de relieve (párrafo 48) que el margen de discrecionalidad del legislador debe interpretarse restrictivamente, al encontrarse comprometidos los derechos a la vida privada y a la protección de datos. De este modo, si bien se considera que la medida resulta idónea para la obtención del fin perseguido, el Tribunal entiende que la misma no supera el juicio de necesidad, al considerar que el objetivo de interés general perseguido no justifica por sí sola la medida de conservación de datos establecida en la Directiva. El Tribunal entiende que el juicio de necesidad no se supera al no cumplirse por la Directiva una serie de medidas que detalla en sus párrafos 51 a 68, referidas resumidamente a la amplitud de la información objeto de tratamiento, la ausencia de controles previos al acceso a la información, la falta de determinación de un plazo de conservación preciso y basado en criterios objetivos, la inexistencia de criterios claros para delimitar las medidas de seguridad que habrán de implantarse en el tratamiento y el hecho de que la Directiva no establece garantías para que los datos almacenados por los operadores no permanezcan en el territorio de la Unión.

- La sentencia de 8 de abril de 2014, dictada en el asunto C 288/12 (Comisión Europea, Supervisor Europeo de Protección de Datos (SEPD) contra Hungría) recalca el requisito de independencia exigible de las autoridades de protección de datos, considerando que Hungría ha vulnerado el derecho de la Unión como consecuencia de la adopción de determinadas reformas legislativas que implicaron en la práctica una reducción del período de mandato del Presidente de su autoridad de control.

- La sentencia de 11 de diciembre de 2014, recaída en el Asunto C 212/13 (František Ryneš y Úřad pro ochranu osobních údajů), que analiza el régimen aplicable a la instalación de dispositivos de videovigilancia que captan imágenes de la vía pública. La sentencia considera que el tratamiento se encuentra sometido a las normas de protección de datos, no siéndole de aplicación la denominada «excepción doméstica». Al propio tiempo se señala que el tratamiento podría encontrarse legitimado por el artículo 7 f) de la Directiva 95/46/CE cuando se lleva a cabo para proteger la persona y bienes de quien instala el dispositivo, si bien será necesario que se respete el principio de proporcionalidad.

3 DESAFÍOS PARA LA PRIVACIDAD: PRESENTE Y FUTURO

A) LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA EN EL CASO GOOGLE SPAIN S. L. Y GOOGLE INC. CONTRA AEPD, MARIO COSTEJA

El 13 de mayo de 2014 el Tribunal de Justicia de la Unión Europea (TJUE) emitió su sentencia en el asunto C-131/12 (Google Spain, S. L., Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), resolviendo la cuestión prejudicial planteada en 2012 por la Audiencia Nacional.

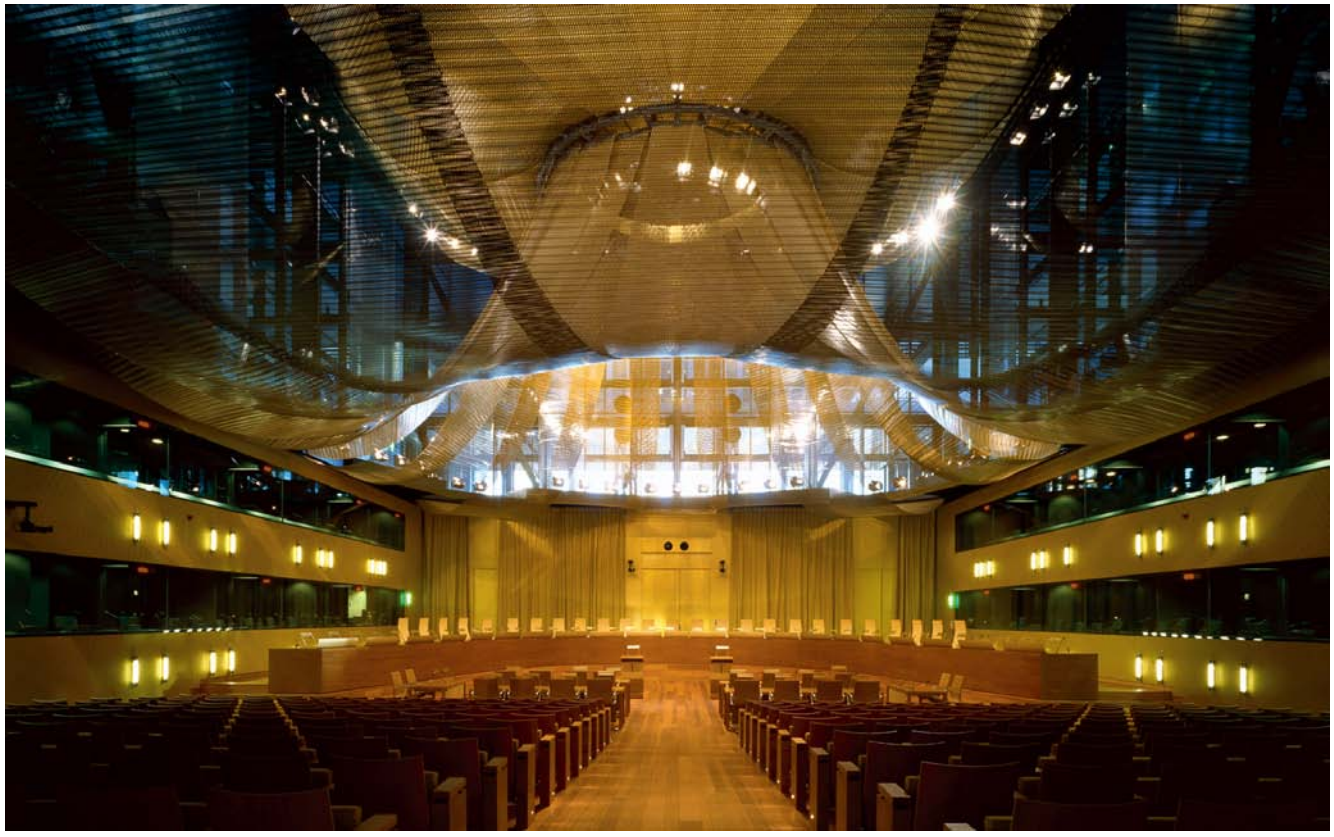
Aunque el origen de este caso es sobradamente conocido, cabe recordar aquí que la Audiencia Nacional planteó la cuestión prejudicial a fin de recabar la interpretación del Tribunal europeo sobre varios apartados de la Directiva 95/46 que resultaban relevantes para la resolución de los más de 200 recursos pendientes ante la Audiencia. Todos estos recursos tenían en común que habían sido interpuestos de forma sistemática por Google contra decisiones de la AEPD en las que esta requería al buscador retirar de su lista de resultados determinados enlaces al realizar la búsqueda mediante el nombre del afectado. Las decisiones de la Agencia, por su parte, respondían a reclamaciones de ciudadanos que habían intentado ejercer ante la compañía sus derechos de cancelación y oposición al tratamiento de sus datos personales sin que esta atendiera sus demandas.

La Audiencia Nacional había planteado al TJUE tres bloques de cuestiones:

- Aplicación de las normas de protección datos de la Unión Europea (en este caso las españolas) a motores de búsqueda que tienen su sede fuera de la UE.
- Posible consideración de la actividad de los buscadores como tratamiento de datos personales y, en su caso, la calificación jurídica de los gestores de los motores de búsqueda como responsables de tratamiento.
- Alcance de los derechos de cancelación y oposición frente a los motores de búsqueda.

En su sentencia, el TJUE hace una interpretación finalista de la noción de establecimiento para concluir que el derecho europeo, y más concretamente la legislación española, son aplicables al motor de búsqueda. El Tribunal considera que la actividad del buscador se enmarca en, y está intrínsecamente vinculada a, la actividad publicitaria que se desarrolla a través del establecimiento que Google tiene en España. Google se rige por un interés económico y la publicidad es la fuente principal, casi exclusiva, de los ingresos que obtiene el motor de búsqueda. En consecuencia, ese establecimiento en España estaría en la situación prevista en el art. 4.1.a de la Directiva 95/46, lo que determinaría la aplicación de la legislación española.

Respecto al segundo grupo de cuestiones, el Tribunal considera que los motores de búsqueda realizan un tratamiento de datos personales. Aunque los datos estén ya en internet y el buscador no los altere, el motor de búsqueda recoge esos datos, los registra y organiza, y finalmente los comunica



G. Fessy ©TJUE

y facilita el acceso a ellos por parte de los usuarios. Operaciones todas ellas que se integran en la definición de tratamiento que ofrece la Directiva.

Al mismo tiempo, el Tribunal concluye que los gestores de los motores de búsqueda actúan como responsables de esos tratamientos, en la medida en que deciden sus fines y medios. El papel del motor de búsqueda es distinto del que desempeña el editor que ofrece originariamente la información en la web. Los fines, medios y consecuencias son distintos.

Respecto al alcance de los derechos de los ciudadanos, debe subrayarse, ante todo, que el Tribunal no reconoce la existencia de un derecho nuevo, el «derecho al olvido». El Tribunal basa toda su argumentación jurídica en los derechos de cancelación y de oposición, aplicando las normas que los regulan.

El TJUE constata que la actividad de los buscadores tiene un impacto significativo sobre los derechos fundamentales del respeto a la vida privada y de protección de los datos personales. Precisamente porque en búsquedas a partir del nombre de una persona se puede obtener una visión completa y estructurada de toda la información existente en internet sobre ella, lo que permite la elaboración de perfiles más o menos detallados. Ese efecto se acentúa por el importante papel que desempeñan

los buscadores. Son la difusión y accesibilidad universales que ofrecen estos las que pueden dar lugar a lesiones sobre los derechos de las personas de una forma mucho más intensa y grave que la publicación original de la información.

El Tribunal no asume la tesis según la cual la actividad del buscador estaría, como tal, legitimada por el ejercicio de la libertad de expresión. Para el Tribunal, el interés legítimo que el buscador puede aducir para desarrollar los tratamientos que realiza es meramente económico y no basta para justificar la grave injerencia sobre los derechos individuales que conlleva. Sin embargo, el Tribunal señala que es preciso considerar también el interés de los usuarios en acceder a la información a través del motor de búsqueda. Con carácter general, los derechos de la persona afectada prevalecerían también sobre ese interés en localizar una información mediante búsquedas nominativas, pero en cada caso específico ese equilibrio dependerá de la ponderación entre la naturaleza de la información de que se trate, de su carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de la información, un interés que puede variar, en particular, en función del papel que esa persona desempeñe en la vida pública.

En todo caso, el interesado que quiera ejercer sus derechos de cancelación o supresión puede hacerlo directamente ante el buscador, sin necesidad de dirigirse previa o simultáneamente al editor original, dado que el tratamiento que el buscador realiza se diferencia nítidamente del que lleva a cabo el editor original y el buscador tiene unas obligaciones como responsable de ese tratamiento que son también distintas de las que tiene el editor.

En la medida en que el Tribunal se remite a derechos existentes como son los de cancelación y oposición, en la ponderación que debe realizarse frente a los intereses de los usuarios del buscador se aplican los criterios que rigen para el ejercicio de esos derechos. Se produce así una diferenciación según la información y según la relevancia pública del afectado. La relevancia, en el momento actual, de la información, su exactitud, el hecho de que haya quedado obsoleta o que resulte incompleta son factores que hay que considerar junto con el papel que el interesado desempeña en la vida pública. Es importante destacar que el Tribunal señala expresamente que no es necesario que se cause un perjuicio para ejercer el derecho frente al buscador.

Con esta sentencia el TJUE corroboraba en todos sus extremos la posición sostenida por la AEPD tanto en las numerosas resoluciones pendientes ante la Audiencia Nacional como durante el procedimiento ante el Tribunal.

La sentencia resuelve las cuestiones presentadas por un tribunal español y es a éste al que corresponde aplicarla en la resolución del litigio que las motivó y en todos los asuntos pendientes de similar naturaleza. Como se ha indicado anteriormente, con posterioridad a la sentencia del TJUE Google desistió de 136 de los recursos planteados ante la Audiencia Nacional, con lo que las resoluciones de la Agencia devinieron firmes. Por otro lado, la Audiencia Nacional dictó en este ejercicio 35 sentencias sobre los recursos interpuestos por la compañía, siendo 24 desestimatorias, 10 estimatorias y una parcialmente estimatoria.

Más allá de la aplicación inmediata de la sentencia, su análisis y conclusiones tienen un valor interpretativo general que se extiende más allá del caso concreto al que se refieren. La consideración de que la actividad de los buscadores constituye un tratamiento, de que los buscadores son responsables y de que cabe ejercer los derechos de cancelación y oposición respecto a ese tratamiento y

<Índice>

en relación a resultados obtenidos a partir de búsquedas realizadas por el nombre de los afectados es válida siempre que se aplica el derecho europeo de protección de datos o, más exactamente, las legislaciones nacionales que lo trasponen a los derechos internos de los Estados miembros. Lo mismo sucede con los parámetros sobre los que deber efectuarse una ponderación entre los intereses de los usuarios del buscador y los derechos e intereses de los afectados.

Ello ha supuesto que en la Unión Europea se haya registrado un aumento notable de las solicitudes de bloqueo de determinados resultados ofrecidos por el buscador cuando se realiza una búsqueda por el nombre del reclamante, que las compañías gestoras de motores de búsqueda hayan tenido que desarrollar procedimientos *ad hoc* para atender estas solicitudes y que Autoridades de protección de datos y tribunales de justicia hayan comenzado a tener que pronunciarse de forma sistemática sobre casos de este tipo.

Para la AEPD la sentencia no plantea nuevos escenarios, dado que se han gestionado solicitudes de tutela de este tipo desde hace varios años y que la sentencia, como se ha señalado, recoge en su totalidad los planteamientos seguidos por la Agencia en la resolución de las solicitudes recibidas. Pero esta experiencia de la AEPD no era compartida por las restantes autoridades europeas, que se han visto obligadas a aplicar unos nuevos criterios que no habían utilizado hasta entonces.

Ello hizo aconsejable que el grupo de Autoridades de protección de datos de los Estados miembros de la UE (GT29) elaborara un documento de guía destinado a establecer las orientaciones básicas para aplicar la sentencia y servir de apoyo a las Autoridades nacionales, así como a las entidades implicadas en su aplicación.

Este documento, en cuya elaboración la AEPD ha actuado como ponente, con el apoyo de las Autoridades de protección de datos francesa y británica, integra directrices que constan de dos partes relacionadas, aunque bien diferenciadas. Una de ellas, la principal, contiene un análisis de las implicaciones tanto teóricas como prácticas de la sentencia. Este análisis podría resumirse en los siguientes puntos:

- Los motores de búsqueda son responsables de tratamiento.

- Los ciudadanos pueden dirigir sus solicitudes directamente a los motores de búsqueda, sin tener que contactar con el responsable de la web original.

- Las decisiones deben tomarse caso por caso, ponderando los diversos derechos fundamentales e intereses afectados.

- El impacto de las decisiones de bloqueo de los enlaces sobre la libertad de expresión es muy limitado, ya que el ejercicio de los derechos de oposición y cancelación sólo afecta a las búsquedas hechas mediante el nombre de la persona afectada, no se borra ninguna información ni de la fuente original ni de los índices del buscador y el bloqueo sólo se produce respecto a informaciones que no tienen interés para el público.

- Las decisiones de borrado deben garantizar la plena protección de los derechos de los interesados. Ello significa que estas decisiones han de producirse en todos los dominios relevantes, incluyendo los «.com», lo cual abarca, en todo caso, aquellos que sean accesibles desde territorio europeo.

- No hay ninguna base legal para informar a los usuarios de que se han bloqueado vínculos específicos.

- El buscador no tiene ninguna obligación legal de contactar con la página web original para informar de que se han bloqueado determinados resultados y la comunicación de que se ha producido ese bloqueo podría ser contraria a la normativa de protección de datos.

La segunda parte del documento contiene una serie de criterios de ponderación que serán aplicados por las Autoridades de protección de datos en la valoración de las reclamaciones que se planteen si los buscadores rechazan las solicitudes de los interesados. Estos criterios reflejan la experiencia común acumulada por las Autoridades del GT29 en el estudio de las primeras solicitudes recibidas después de la sentencia. Entre ellos se incluyen, por ejemplo, el papel que el interesado juega en la vida pública, el carácter sensible para la privacidad de las informaciones afectadas, la posible minoría de edad del afectado, la existencia o no de obligaciones legales de publicar las informaciones, etc.

B) EL RESPETO A LA PRIVACIDAD COMO LÍMITE DE LAS AUTORIDADES: EL TRATAMIENTO DE DATOS DE PASAJEROS (PNR)

En los primeros días de enero de 2015 se produjeron graves atentados terroristas en París contra el semanario satírico Charlie Hebdo y contra establecimientos de la comunidad judía.

Dado que, según todas las evidencias, los autores de estos ataques tenían conexiones con bases terroristas en Oriente Medio y habían viajado allí para recibir entrenamiento, muchos responsables políticos se manifestaron inmediatamente a favor de adoptar medidas para mejorar el control de las fronteras europeas y, en particular, de relanzar y concluir rápidamente el proceso de aprobación de la Directiva sobre un PNR europeo.

Se reabrían así los debates sobre un tema, el del tratamiento de datos de viajeros, que refleja la compleja relación que mantienen seguridad y derechos y libertades fundamentales. Debates que, sin duda, van a continuar en los próximos años con respecto a datos PNR, pero también en el creciente número de ámbitos en que las exigencias de seguridad determinan el tratamiento de datos personales.

La denominación PNR (Passenger Name Record) corresponde realmente a los registros que las compañías aéreas o sus agentes crean para cada viaje y viajero y que se almacena en los sistemas de reservas y control de salidas de esas compañías. Cada registro contiene un número normalizado de categorías de datos, e incluye toda la información que la compañía aérea precisa para poder prestar su servicio de transporte.

A partir de 2001, las autoridades policiales empezaron a requerir a las compañías que les enviasen, con antelación a la salida de cada vuelo, algunos de los datos contenidos en el PNR para todos los vuelos internacionales que se dirigieran a, o que partieran de, un determinado país. Por ello, cuando se habla de datos PNR o de PNR en el contexto de protección de datos, se entiende que se alude a la comunicación a las fuerzas de seguridad de estos datos, recogidos y tratados originariamente para los fines propios del servicio que prestan las compañías aéreas, con finalidades relacionadas con la lucha contra el terrorismo u otras formas de delincuencia transnacional.

El primer esquema de PNR fue implantado por Estados Unidos, y le siguieron los de Canadá y Australia. Posteriormente, otros países de todo el mun-

<Índice>

do, incluidos algunos de la Unión Europea, han establecido, o han anunciado que establecerán, sistemas similares.

La generalización de estos usos de los datos PNR puede atribuirse a la confluencia de dos tipos de factores. De un lado, el rápido desarrollo tecnológico, que ha permitido recoger, almacenar y procesar con gran eficacia información relativa a una gran variedad de aspectos de la vida de los ciudadanos en unas magnitudes antes impensables y con unos costes también mucho más bajos que en un pasado relativamente reciente. De otro, las autoridades policiales y de seguridad, enfrentadas al crecimiento y la sofisticación de los tipos de delincuencia mencionados, buscan desarrollar nuevos métodos para combatirlos.

La Unión Europea buscó incorporarse al grupo de países demandantes de datos PNR, y ya en 2007 la Comisión presentó una propuesta de Decisión Marco sobre la utilización de datos PNR. Durante la tramitación de esa propuesta entró en vigor el Tratado de Lisboa, por lo que fue preciso sustituirla por otra más adecuada al nuevo marco legal, presentándose en 2011 una propuesta de Directiva de PNR Europeo con finalidades similares.

La nueva propuesta, según señalaba la Comisión en su memoria explicativa, obedecería, por una parte, a la necesidad de responder a las amenazas contra la seguridad derivadas de los delitos terroristas o de otros delitos graves. Esta necesidad habría sido confirmada, también según la memoria explicativa, «por la información procedente de los terceros países y los Estados miembros que ya utilizan datos PNR con fines coercitivos».

Al tratarse de una Directiva, la memoria explicativa señalaba que su adopción tiene por objeto la armonización de las disposiciones nacionales sobre PNR en toda la Unión, si bien reconocía que sólo unos pocos Estados miembros lo utilizaban en ese momento, mientras que otro grupo, también reducido, estaría planteándose su puesta en marcha.

La propuesta de Directiva fue objeto de informes muy críticos tanto por parte del Supervisor Europeo de Protección de Datos, en el desempeño de sus funciones consultivas en los procesos normativos de la Unión, como del Grupo de Autoridades de protección de datos de los Estados miembros (GT29). En los dos casos, el principal motivo de crítica se refería al incumplimiento de los principios de necesidad y proporcionalidad en este tratamiento adicional de los datos PNR, que supone una seria interferencia sobre derechos de los ciudadanos expresamente recogidos en el Convenio Europeo de Derechos Humanos y la Carta Europea de Derechos Fundamentales como son el derecho a la privacidad y el derecho a la protección de datos.

Desde esta óptica, el Dictamen del GT29 sobre el PNR europeo apunta en primer lugar a un cuestionamiento general que se puede resumir en que ninguna autoridad de protección de datos ha tenido evidencia de que el tratamiento de cantidades masivas de datos (la Directiva prevé que se recojan 19 categorías de datos, algunas de las cuales incluyen, a su vez, subconjuntos de datos) sobre todos los pasajeros resulte necesario, esto es, suficientemente eficaz y en un modo en que no podría obtenerse por otros medios menos invasivos, y proporcionado para el logro de las finalidades perseguidas.

El Grupo critica también que la Comisión Europea no proporcionase resultados de evaluación de programas ya existentes que contemplan la recogida de información y su intercambio entre autoridades policiales europeas con finalidades policiales, incluida la lucha contra el terrorismo. Sin tener una evaluación formal de la eficacia de esos programas

no es posible juzgar si el PNR satisface criterios de necesidad y proporcionalidad en el sentido de no ser sustituible por otras medidas igualmente eficaces pero de menor impacto.

El Dictamen apunta también a problemas derivados de la definición imprecisa de las finalidades, así como con el uso que se hace de los datos por las autoridades receptoras. La Directiva prevé, por ejemplo, que los datos puedan ser cruzados «con otras bases de datos pertinentes» o que se compararán con «criterios predeterminados». En ambos casos hay dudas sobre la extensión de los correspondientes tratamientos y su relación con la finalidad perseguida, dado que no se establece de un modo exhaustivo cuáles pueden ser las bases que se consultarían ni tampoco se definen esos criterios o cómo han podido ser desarrollados.

Se considera, igualmente, que no queda establecida la necesidad de tratar todos y cada uno de los datos que se transmiten para cada pasajero, sea o no sospechoso. La falta de evidencia de la necesidad de tratar toda la información de todos los viajeros genera un problema de proporcionalidad. Sobre todo en relación con otros aspectos como pueden ser las cesiones ulteriores o los largos periodos de retención.

El Dictamen, por último, no considera suficientemente establecido que haya necesidad, y que sea proporcionado, que todos los datos de todos los viajeros se conserven durante los largos plazos de retención previstos que, aparentemente, se fijan de un modo relativamente arbitrario, como parece indicar que diferentes PNR hayan tenido en el pasado periodos de retención más o menos largos.

Adicionalmente, el documento también critica otros elementos de la propuesta como la regulación de las cesiones dentro de cada Estado miembro, entre Estados miembros y a autoridades de países terceros.

La propuesta de Directiva se tramita por el procedimiento legislativo ordinario, con participación del Consejo y el Parlamento Europeo. En 2013, la propuesta quedó bloqueada en el Parlamento, cuando fue rechazada por su Comisión LIBE. El principal argumento de los eurodiputados contrarios a la aprobación se basaba también en sus dudas sobre la necesidad y proporcionalidad del sistema propuesto. Ante la falta de acuerdo entre los grupos, el pleno decidió remitir el asunto nuevamente a la LIBE.

Tras el bloqueo en el Parlamento, en 2014 se han producido otros hechos que pueden tener incidencia en la suerte que finalmente pueda correr el PNR europeo.

Por un lado, el 8 de abril de 2014, el Tribunal de Justicia de la Unión Europea (TJUE) emitió una sentencia (que se encuentra detallada en el apartado *La seguridad jurídica como objetivo primordial* de esta Memoria) resolviendo una cuestión preliminar planteada en relación con la validez de la Directiva 2006/24/CE de retención de datos de tráfico de las telecomunicaciones. La Directiva establecía la obligación de que los operadores conservaran una serie de datos de tráfico por un periodo entre 6 meses y 2 años para ponerlos a disposición de las autoridades competentes con finalidades de investigación, detección y persecución de delitos graves. En su sentencia, el Tribunal concluyó que la Directiva implicaba una grave interferencia con los derechos fundamentales a la protección de datos y la privacidad. Tal interferencia sólo está permitida cuando resulta necesaria en un estado democrático para el logro de unos fines superiores y siempre que resulte proporcionada al logro de esos fines. El Tribunal declaró no válida la Directiva, por en-

<Índice>

tender que las medidas que establecía no estaban suficientemente restringidas a lo que podría entenderse como estrictamente necesario, y tampoco definía suficientemente las garantías necesarias en relación con la conservación de los datos.

Las similitudes entre la Directiva sobre retención de datos de tráfico de telecomunicaciones y la Directiva PNR son notorias. En ambos casos se produce una recogida masiva de una gran cantidad de datos personales, relativos a todos los usuarios de un determinado servicio, que se almacenan por largos periodos de tiempo y con finalidades de lucha contra formas graves de criminalidad. En ninguno de los dos casos se distingue entre personas que por algún motivo puedan resultar de interés para las autoridades de seguridad y personas sobre las que, como dice el TJUE, «no hay evidencia que pueda sugerir que su conducta podría tener un vínculo, siquiera indirecto o remoto, con delitos graves».

Este paralelismo no ha pasado desapercibido ni en la doctrina, ni en la valoración de las autoridades de protección de datos ni, incluso, en las instituciones comunitarias. Así, el Parlamento Europeo decidió en noviembre de 2014 pedir al TJUE un dictamen sobre la compatibilidad del Acuerdo PNR entre la UE y Canadá con los Tratados de la Unión. El Acuerdo sometido a la consideración del Parlamento pretendía la renovación del vigente entre 2005 y 2009, cuyos efectos fueron prorrogados hasta la adopción del nuevo acuerdo. El Parlamento «considera que existe incertidumbre jurídica sobre la compatibilidad del proyecto de Acuerdo con las disposiciones de los Tratados (artículo 16 del TFUE) y de la Carta de los Derechos Fundamentales de la Unión Europea (artículos 7, 8 y 52, apartado 1) por lo que respecta al derecho de las personas a la protección de sus datos personales (…)». Significativamente, entre los considerandos con los que motiva su decisión, se cita de manera expresa la Sentencia del TJUE sobre la Directiva de retención de datos de tráfico y se alude a los dictámenes del Supervisor Europeo y del GT29 sobre los programas PNR de países terceros.

Ciertamente, esta consulta trata del sistema PNR de un país tercero, pero el Parlamento parece dar a entender que la Sentencia del TJUE contiene elementos que podrían ser aplicables a cualquier esquema de recogida y tratamiento masivos e indiscriminados de datos personales, lo que incluiría el PNR europeo. Máxime cuando el Parlamento ya se había pronunciado en contra del mismo en 2013.

La reacción frente a los atentados en París planteando la adopción del PNR europeo como una prioridad resulta preocupante desde la perspectiva de las Autoridades europeas de protección de datos. Es evidente que unos sucesos tan terribles, que se unen a otros vividos en los últimos años en otros países, exigen respuestas adecuadas y un fortalecimiento de las medidas de prevención y de reacción. Pero de nuevo es preciso valorar esas medidas desde la óptica de los principios de necesidad, de eficacia de las acciones para el logro de los fines perseguidos, y de proporcionalidad, de modulación de las medidas de forma que supongan el mínimo impacto imprescindible en los derechos individuales.

Las Autoridades de protección de datos, como se ha indicado anteriormente, han expresado repetidamente sus dudas sobre la eficacia de posibles programas de PNR tanto a nivel europeo como nacional. Así, es necesario insistir en la pregunta clave de hasta qué punto la recogida de una enorme cantidad de datos de todos los viajeros que vuelan desde o hacia un país, o desde o hacia la Unión Europea, puede contribuir a prevenir atentados terroristas o delitos graves con mayor eficacia de la que ofrecen otros instrumentos que ya están al alcance

de las autoridades. Las evidencias disponibles no avalan, en principio, tal conclusión. En realidad, los sucesos de París parecen apuntar en otro sentido. Los autores eran conocidos de las autoridades, que sabían, a partir de la utilización de los recursos actualmente disponibles, que habían viajado fuera de la Unión Europea con destino a campos de entrenamiento terrorista en Oriente Medio.

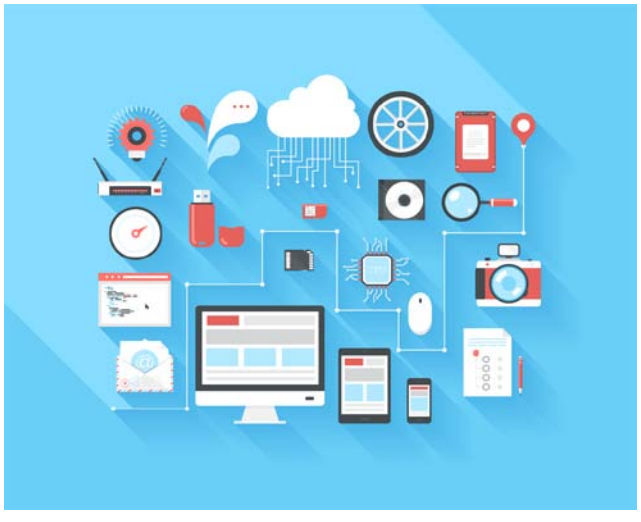
Esta valoración fue reiterada por el GT29 en su primera reunión de 2015, aprobando una Declaración en la que, aparte de reiterar los argumentos expuestos, manifestaba su disposición a colaborar con las instituciones europeas en el desarrollo de medidas en la línea del PNR, pero más ajustadas a las exigencias del ordenamiento europeo. Seguridad y protección de datos no son conceptos opuestos ni contradictorios, pero es preciso encontrar un equilibrio entre ambos.

C) EL INTERNET DE LAS COSAS (IoT)

El año 2014 ha sido caracterizado por muchos agentes como el año del despegue definitivo del Internet de las Cosas, el año en que esta tecnología ha empezado a integrarse, de forma definitiva, como parte de la actividad diaria de los ciudadanos. Así, en paralelo al desarrollo de numerosas iniciativas públicas y privadas se han empezado a introducir en el léxico común conceptos como contador o termostato inteligente, tecnología vestible o *wearable*, ciudades inteligentes y otros muchos relacionados no sólo con el entorno sino con nuestra propia actividad individual, sea profesional, familiar o de ocio.

El fenómeno del Internet de las Cosas no es un fenómeno aislado, sino que forma parte de un conjunto de desarrollos tecnológicos y sociales de amplio alcance que aprovechan las sinergias derivadas de su uso conjunto para alcanzar un mayor grado de eficiencia y que se caracterizan, en todos los casos, por centrar en los tratamientos masivos de datos el eje central de su actividad. En este sentido, el Internet de las Cosas no puede ser adecuadamente entendido sin considerar la influencia del Big Data o del Open Data, así como de las tecnologías que facilitan el desarrollo de la computación en la nube, aquellas especializadas en extraer valor añadido del análisis de cantidades ingentes de información o los nuevos desarrollos en telecomunicaciones capaces de gestionar un mayor ancho de banda de forma más eficiente.

Atisbar lo que puede representar el Internet de las Cosas en un futuro cercano implica asumir la posibilidad de que muchos de los objetos que nos rodean e incluso los propios ciudadanos se conviertan en nodos de una inmensa red de intercambio de información a la que se puede acceder desde cualquier lugar y que se alimenta con los datos generados por la interacción entre dichos nodos, y entre ellos y el entorno en que se ubican. Más allá del ejemplo del frigorífico conectado a internet, se trata de imaginar objetos de uso y presencia cotidiana en nuestras vidas –nuestro vehículo, los elementos de la red de alumbrado de nuestra ciu-



<Índice>

dad– capaces de interactuar con su entorno próximo, reaccionar a ciertos eventos con diverso grado de autonomía, y, sobre todo, compartir flujos de información con otros nodos. En un paso subsiguiente, la información así acumulada puede ser objeto de análisis a nivel agregado o individual con el fin de alimentar diversos sistemas, incluyendo los de toma de decisiones, sean estas de carácter general o afectando a individuos específicos. A mayor cantidad de objetos conectados, mayor volumen de información tratada y mayor posibilidad de establecer relaciones e inferencias basadas en la interacción continuada de los elementos de la red.

Aunque el desarrollo de tecnologías y servicios apoyados en el despliegue del Internet de las Cosas presenta a priori beneficios desde el punto de vista del desarrollo económico y social, es indudable que resulta indispensable lograr el necesario equilibrio entre esos beneficios y la necesaria protección de los datos de carácter personal y la intimidad de los ciudadanos, cuestión ésta que presenta facetas complejas. Así, en la medida en que los individuos puedan percibir que este nuevo entorno representa un riesgo cierto de ser observados de forma continua, a la vez que se queda sujeto a tratamientos de información personal sobre los que no tiene control o este es solo aparente, estos sistemas podrían ser considerados de forma negativa por sus usuarios, poniendo en riesgo que puedan ser usados en todo su potencial y limitando, por tanto, las ventajas de su uso generalizado[1]. Por otro lado, el individuo, incluso plenamente consciente de los beneficios ofrecidos por una tecnología o servicio específico, puede decidir libremente, por una u otra razón, no utilizarlo en todo el rango de posibilidades ofrecidas. Esto, traducido en el ámbito de la protección de datos de carácter personal, implica que el usuario debe mantener en todo momento el control sobre los tratamientos realizados con sus datos.

La Comisión Europea presentó en febrero de 2013 los resultados de una consulta[2] pública sobre el gobierno del Internet de las Cosas cuyo contenido referido a protección de datos e intimidad traslucía un cierto grado de divergencia entre la posición de los promotores de este tipo de servicios y la de las organizaciones de consumidores y usuarios en lo tocante a la necesidad y oportunidad de adaptar el marco legal vigente en protección de datos a esta nueva realidad. El mismo estudio mostraba que la mayoría de los participantes insistía en la necesidad de mantener el poder de control del individuo sobre el tratamiento de sus datos, así como el papel primordial del consentimiento: el usuario debe poder elegir si forma parte o no de un sistema integrado en el Internet de las Cosas. Otras sugerencias incluidas en la consulta apuntaban al papel de primer orden que deben desempeñar los procedimientos de evaluación de impacto sobre la privacidad y la protección de datos, las técnicas de disociación que favorezcan la separación efectiva de la identidad del usuario del conjunto de los datos tratados, así como las medidas de seguridad –con un papel relevante de las técnicas de cifrado–, la transparencia y el estricto control sobre la adecuación del tratamiento a la finalidad declarada del mismo.

Por su parte, las Autoridades de protección de datos de los Estados miembros de la UE (GT29) incorporaron a su programa de trabajo para el año 2014 el estudio detallado de este fenómeno, adoptando un Dictamen[3], presentado el 16 de septiembre, en

[1] De acuerdo a la ley de Metcalfe, el valor de una red aumenta proporcionalmente al cuadrado del número de usuarios.

[2] https://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

el que, utilizando algunos de los desarrollos más recientes en dicho ámbito, se presentaba un análisis general de las implicaciones de este fenómeno, incluyendo los riesgos en protección de datos de carácter personal. El documento también desarrollaba un conjunto de recomendaciones dirigidas a los diversos actores con interés en la puesta en marcha de sistemas integrados en el Internet de las Cosas. En la elaboración de este Dictamen la Agencia Española de Protección de Datos actuó como ponente junto con Comisión Nacional de Informática y Libertades francesa (CNIL).

El Dictamen define el Internet de las Cosas como la infraestructura global en la que sensores con capacidad de interacción con otros sensores y con la realidad circundante se incorporan a dispositivos de uso cotidiano de forma que recogen, tratan, almacenan y transfieren datos utilizando capacidades de interconexión en red. Dado que el todavía incipiente desarrollo del Internet de las Cosas hace imposible prever todas sus posibles manifestaciones y las correspondientes implicaciones, el Dictamen opta por centrar su análisis en tres tipos de tecnologías: los dispositivos de tecnología vestible, los que permiten cuantificar la actividad de la persona y aquellos otros asociados a sistemas de domótica.

El documento trata de identificar los riesgos en materia de protección de datos, haciendo hincapié en la falta de control sobre el tratamiento por parte de los usuarios, la dificultad para obtener el consentimiento informado, la posibilidad de realizar inferencias y adoptar decisiones mediante procedimientos automatizados, el posible desvío de finalidad en los tratamientos, la oportunidad de someter al individuo a una monitorización constante con posible impacto sobre su conducta habitual, así como las debilidades en materia de seguridad derivadas de una escasa atención a este crucial aspecto durante el desarrollo de los productos o de la dificultad de incorporar salvaguardas con impacto en la capacidad de computación del dispositivo o en el consumo de energía.

En todos los casos, los riesgos examinados, que siguen un patrón similar al de otras tecnologías actualmente en desarrollo, permiten identificar rasgos específicos derivados de la propia naturaleza del Internet de las Cosas. Por ejemplo, en lo que se refiere al derecho de información, se evidencia la complejidad de ofrecer al usuario la información relevante a sus intereses en unos soportes que pueden ser de muy pequeño tamaño o estar incorporados en otros dispositivos y que, en todo caso, pueden llegar a tener una presencia tan abrumadora que haga prácticamente inviable que el usuario gestione toda la información recibida.

Por lo que se refiere a la seguridad, las exigencias de tamaño, consumo de energía, autonomía y eficacia propias de los objetos que han de integrarse en los sistemas del Internet de las Cosas son, en estos momentos, en buena medida difícilmente compatibles con los requisitos de implantación de medidas de seguridad que son habituales en sistemas de mayor tamaño y capacidad de computación. En ese sentido, y aun reconociendo el notable avance en este ámbito, todavía se está lejos de alcanzar una solución viable en el desarrollo de técnicas de cifrado y control de acceso compatibles con un uso reducido de recursos de computación. Por otro lado, la dispersión en la responsabilidad del desarrollo de distintos componentes de los componentes físicos y lógicos asociados a un objeto hacen difícil para el integrador de estos mantener un control preciso sobre la seguridad de cada uno de ellos en un único sistema, con el resultado final de que la seguridad global del dispositivo es equivalente a la del componente que presente una mayor debilidad en ese aspecto.

<Índice>

El Dictamen subraya igualmente el hecho de que el Internet de las Cosas comparte con otros desarrollos tecnológicos de nueva factura la existencia de una pluralidad de actores interesados en extraer valor añadido de los tratamientos de datos realizados. El documento identifica a los fabricantes de los dispositivos, desarrolladores de aplicaciones, plataformas sociales o intermediarios de datos como agentes con un papel activo en la recogida, procesamiento y ulterior distribución de datos de carácter personal. Por ello, las recomendaciones contenidas en el Dictamen se dirigen separadamente a cada uno de estos grupos, girando en torno a la idea central de que los usuarios deben conocer y mantener el control de sus datos personales a lo largo de todo el ciclo de tratamiento.

Cuando las organizaciones basen los tratamientos de datos en el consentimiento, ese consentimiento debería ser libre, específico y plenamente informado. De esta forma, y aun reconociendo la dificultad de una correcta gestión del consentimiento en este nuevo entorno utilizando procedimientos tradicionales, en el Dictamen se hace una defensa fundada de su validez como base legal para el tratamiento y se aboga por el desarrollo de soluciones novedosas que permitan conciliar las necesidades de eficiencia en el despliegue y uso de los sistemas del Internet de las Cosas con los derechos individuales.

Por otro lado, y considerando las herramientas a disposición de los responsables del tratamiento, el Dictamen insiste en la necesidad de utilizar técnicas que favorezcan la correcta aplicación de los principios de privacidad desde el diseño y de privacidad por defecto, en particular la evaluación de impacto en la protección de datos. Esta herramienta, cuyos antecedentes en el ámbito del Internet de las Cosas se remontan a la Recomendación de la Comisión Europea sobre identificadores de radiofrecuencia de 2009[4], de la que se deriva el desarrollo de un marco de evaluación de impacto sobre protección de datos específico de esta tecnología[5], se proyecta como una metodología adecuada para ser utilizada en otros ámbitos como el despliegue de redes inteligentes de suministro eléctrico o en el uso de tecnologías de la información en la salud.

Así, en lo tocante a las redes de suministro eléctrico y contadores inteligentes, el Reglamento 2012/148/UE relativo a los preparativos para el despliegue de los sistemas de contador inteligente, requiere tanto de los Estados miembros como de los operadores de redes y sistemas de contador inteligente adoptar un conjunto de medidas. Entre ellas se encuentra el desarrollo de un modelo de evaluación de impacto sobre la protección de los datos adaptado a estos sistemas, que ha cristalizado en la Recomendación 2014/724/UE de la Comisión Europea, de 10 de octubre de 2014[6], relativa al modelo de evaluación de impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente[7], que ofrece orientaciones sobre su aplicación en el desarrollo de ese tipo de infraestructuras.

Una última referencia al Dictamen del GT29 nos conduce a las recomendaciones dirigidas a los organismos internacionales de estandarización en el sentido de promover estándares interoperables con el fin de facilitar la transferencia de informa-

---

[4] Es interesante señalar que a mediados de 2014 la Comisión Europea anunció un acuerdo sobre nuevos estándares técnicos paneuropeos para garantizar que los chips y sistemas RFID cumplen las normas de protección de datos de la Unión Europea y la Recomendación de mayo de 2009.

[5] Norma española EN 16571:2014: Tecnología de la información. Proceso de evaluación del impacto de la privacidad RFID (PIA).

[6] http://www.boe.es/doue/2014/300/L00063-00068.pdf

[7] https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

ción entre los diferentes agentes participantes en un sistema integrado en el Internet de las Cosas, a la vez que se permite a los titulares de los datos entender qué tratamientos se están realizando. Estos estándares, que deberían permitir la certificación por parte de entidades independientes, han de considerar elementos como las estructuras y formatos de intercambio de datos, el tratamiento de información agregada así como, centrándonos en el ámbito de la seguridad y las comunicaciones, el desarrollo de protocolos de cifrado y comunicación adaptados a las limitaciones presentes en los dispositivos utilizados en estas soluciones, en particular la capacidad limitada de computación y la autonomía de funcionamiento.

Es evidente que, si se da crédito a las previsiones que, casi a diario, son publicadas sobre el despliegue –fulgurante– del Internet de las Cosas, tiene sentido considerar que dichas tecnologías van a tener un claro impacto en la vida diaria de los ciudadanos en los próximos años. Subsisten numerosos interrogantes en lo tocante a la capacidad de poner en marcha las infraestructuras necesarias, en el ritmo de adopción o, simplemente, sobre si la aceptación por parte del usuario va a ser la esperada por los promotores de estos sistemas. En todo caso, no hay duda de que el Internet de las Cosas, en combinación con otros desarrollos como el Big Data y la computación en la nube, va a tener un papel creciente en la actividad de supervisión de las Autoridades de protección de datos en los próximos años, tanto a nivel nacional como de la Unión Europea. En ese ínterin, seguimos caminando hacia lo que ya se conoce como el Internet de todas las cosas, donde los objetos *adquieren conciencia* de su contexto, y gestionan una mayor potencia de procesamiento y una mayor y mejor capacidad de detección de su entorno, aprendiendo en última instancia, a decidir por sí mismos.

D) BIG DATA

Big Data o Datos Masivos es un término que hace referencia al enorme incremento en el acceso y uso automatizado de información. Se refiere a las gigantescas cantidades de datos digitalizados que son controlados por las empresas, autoridades públicas y otras grandes organizaciones que poseen la tecnología para realizar un análisis extenso de los mismos basado en el uso de algoritmos.

Es innegable que los datos masivos pueden ser una fuente de innovación y de nuevo valor económico. Pueden tener aplicación en una gran variedad de ámbitos, no sólo para definir hábitos de consumo o crear perfiles de consumidores sino en el ámbito de la seguridad nacional, la investigación científica, los estudios médicos, la prevención de catástrofes naturales o de propagación de enfermedades, la persecución del fraude fiscal, etc. Pero estos avances entrañan también importantes riesgos para la privacidad de los ciudadanos que deben ser valorados con el fin de garantizar su derecho a la protección de datos personales.

La Agencia está prestando especial atención al desarrollo de esta tecnología, que va a ser sin duda uno de los grandes retos de los próximos años. Así, además de trabajar internamente para evaluar sus implicaciones en materia de protección de datos, la AEPD ha sido partícipe en el ámbito internacional de los dictámenes y documentos de trabajo elaborados conjuntamente para analizar este fenómeno.

El Big Data implica el tratamiento de distintas categorías de datos: estructurados, semiestructurados y no estructurados:

- La mayoría de las fuentes de datos tradicionales dan lugar a datos estructurados. Se trata de datos con formato o esquema que poseen campos fijos, como los de las bases de datos

<Índice>

relacionales, las hojas de cálculo y los archivos, fundamentalmente. Algunos formatos típicos son fecha de nacimiento (DD/MM/AA), el DNI o pasaporte (dígitos y una letra) o número de cuenta corriente bancaria (20 dígitos).

- Los datos semiestructurados no tienen formatos fijos pero contienen etiquetas y otros marcadores que permiten separar los elementos que contienen datos. Su lectura requiere el uso de reglas complejas que determinan cómo proceder después de la lectura de cada pieza de información. Un ejemplo de esta categoría son los registros *web logs* de las conexiones a internet. Un *web log* se compone de diferentes piezas de información, cada una de las cuales sirve para un propósito específico. Otros ejemplos típicos son el texto de etiquetas de XML y HTML.

- Los datos no estructurados son datos sin tipos predefinidos. Se almacenan como objetos o documentos sin una estructura uniforme. Ejemplos de ello son las piezas de audio, de vídeo, las fotografías o formatos de texto libre como correos electrónicos, mensajes SMS, artículos, libros, mensajes de mensajería instantánea tipo Whatsapp, Viber, etc. Se calcula que al menos el 80% de la información de las organizaciones son datos no estructurados.

Si unimos a los datos tradicionales o estructurados los nuevos datos procedentes de sensores, entradas (*posts*) en redes sociales, imágenes digitales, vídeos y fotos, registros de transacciones comerciales y bancarias, señales GPS de los móviles, registros de servidores web, imágenes de satélites, contenido de las páginas web, documentos de la Administración pública (Open Data), historial de pulsaciones (clics), incidencias telefónicas, etcétera, nos encontramos con una ingente cantidad de datos que crecen cada día y que pueden ser captados, almacenados, procesados y analizados.

Las características que definen al Big Data son las denominadas «tres Vs»: volumen, velocidad y variedad.

En cuanto al volumen de información, este ha aumentado tanto que el cambio cuantitativo ha conducido a un cambio cualitativo. Las organizaciones tratan volúmenes masivos de datos, de forma que ampliando la escala de los datos se pueden obtener nuevos resultados a los que no se podía llegar cuando sólo se trabajaba con cantidades más pequeñas de información.

La importancia de la velocidad de los datos o el aumento creciente de los flujos de información en las organizaciones, sumado a la frecuencia de las actualizaciones de las grandes bases de datos, son características importantes a tener en cuenta. Estas circunstancias requieren que el procesamiento y posterior análisis normalmente ha de hacerse en tiempo real para mejorar la toma de decisiones sobre la base de la información generada.

A estas características, algunos investigadores añaden dos variables adicionales: el valor y la veracidad («5 Vs»).

Con el Big Data, la información se ha convertido en el objeto mismo de intercambio y han adquirido mayor un valor. Este valor reside no sólo en su uso primario sino en sus potenciales usos futuros. Los datos pueden ser explotados con propósitos múltiples y su valor pleno es mucho mayor que el que se obtiene de su primer uso. Así, los datos pasan de unos usos primarios a otros potenciales secundarios, lo que los vuelve mucho más valiosos a lo largo del tiempo ya que la información generada para un propósito concreto se reutilizará para otro.

3

Por su parte, la veracidad está asociada a los niveles de fiabilidad de los datos objeto de tratamiento por lo que es necesario intentar conseguir información de calidad. Por ello, alcanzar un alto nivel de veracidad o fiabilidad en el Big Data supone un gran reto que aumenta a medida que la variedad y las fuentes de datos crecen.

En lo que respecta a la utilización de técnicas de Big Data, esta está relacionada con el tratamiento de ingentes cantidades de datos a los que se aplica algoritmos con el fin de establecer correlaciones entre ellos y elaborar perfiles o patrones que permitan hacer predicciones sobre el comportamiento futuro de las personas y tomar decisiones basadas en esas predicciones, lo que se denomina analítica predictiva.

La analítica predictiva es una tecnología que aprende de la experiencia (los datos) para predecir el futuro comportamiento de los individuos con el fin de tomar mejores decisiones. En este sentido, los datos masivos tratan de obtener resultados sobre qué está ocurriendo o va a ocurrir, pero no por qué se ha producido o se va a producir.

La generalización de decisiones tomadas únicamente partiendo de un análisis predictivo puede tener consecuencias adversas para los ciudadanos, dando lugar a la consolidación de prejuicios y estereotipos preexistentes y al crecimiento de la exclusión y la desigualdad social.

La era de los datos masivos puede llegar a alterar el funcionamiento de los mercados y la sociedad conduciéndonos a la llamada «dictadura de los datos» (Viktor Mayer-Schönberger) y supone un reto para las Autoridades encargadas de velar por la protección de este derecho fundamental anticiparse a las demandas de los ciudadanos para salvaguardar su privacidad en este nuevo contexto.

La toma de decisiones basadas en Big Data podría incrementar el desequilibrio de poder (*power imbalance*) entre las grandes empresas y corporaciones, por un lado, y los consumidores, por otro, así lo señala el GT29 en su Dictamen 3/2013.

Son las empresas que recopilan datos personales las beneficiarias en primer término del valor inherente de esos datos analizados y procesados, y no los consumidores que los han proporcionado. Además, esta transacción de datos coloca al consumidor en situación de desventaja en el sentido de exponerle a potenciales futuras vulnerabilidades. Baste pensar en una situación en la que se aplique el tratamiento de datos masivos en relación a las oportunidades de encontrar un empleo, obtener una hipoteca u otro préstamo bancario o contratar un seguro médico. Estaremos ante decisiones que pueden perjudicar al ciudadano y que se toman sobre la base de una información que muchas veces éste desconoce que ha facilitado.

Los interrogantes que el uso de Big Data abre en el ámbito de la protección de datos personales son muy diversos: la obtención del consentimiento, el ejercicio de los derechos de información y acceso,

rectificación, cancelación u oposición, la correcta anonimización de los datos antes de analizarlos, el desvío de la finalidad para la que fueron recogidos y otras posibles vulneraciones del principio de calidad de los datos (datos inexactos o excesivos) o riesgos relacionados con la re-identificación en el tratamiento de datos anonimizados.

Así lo entiende el Grupo Internacional de Trabajo sobre Protección de Datos en el sector de las Telecomunicaciones (Grupo de Berlín), que en 2014 ha elaborado un documento de trabajo sobre Big Data y privacidad (*Privacy principles under pressure in the age of Big Data analytics*).

El Grupo de Berlín destaca una serie de principios clave cuyo respeto y observancia es especialmente relevante en el ámbito de Big Data:

- Principio de legitimidad y consentimiento: para que el tratamiento del dato personal sea legítimo el afectado ha de prestar su consentimiento inequívoco.
- Principio de limitación de la finalidad: los datos han de ser utilizados sólo para la finalidad para la que fueron recabados.
- Principio de calidad: datos adecuados, pertinentes, no excesivos, exactos y actualizados.
- Principio de minimización de los datos: datos no excesivos, utilizar sólo los datos necesarios para cumplir el fin con el que se recaban y no más.
- Principio de información o transparencia: derecho del ciudadano de conocer y acceder a toda la información que se posea sobre él mismo.

De igual forma, el GT29 se ha pronunciado en 2014 acerca del impacto del desarrollo del Big Data en relación con el tratamiento de los datos personales en la UE (WP 221). Esta Declaración es la primera toma de posición específica del Grupo sobre el fenómeno del Big Data, aunque otros documentos anteriores, como el relativo a anonimización, ya lo trataban de forma indirecta.

El Grupo parte de considerar que, en la medida en que una parte importante de las operaciones de Big Data se basan en un tratamiento masivo de datos personales de ciudadanos en la UE, se plantean importantes cuestiones sociales, legales y éticas entre las que figuran las que tienen que ver con la privacidad y la protección de datos de los ciudadanos.

Frente a las críticas que cuestionan la validez de principios básicos de protección de datos como el de limitación de finalidad o minimización de datos en el contexto del Big Data, el Grupo sostiene que por ahora no ve motivos para pensar que estos principios, adecuadamente actualizados, no sean válidos y apropiados para el desarrollo de esta tecnología. Al mismo tiempo, subraya que los principios de protección de datos son aplicables a todas las operaciones de tratamiento, desde el momento de la recogida y siempre con la finalidad de conseguir un elevado nivel de protección.

El Grupo reconoce también que el carácter global de los procesos de Big Data supone la aplicación simultánea de diversos regímenes legales y que, por ello, la cooperación entre las autoridades europeas y otras autoridades, tanto de protección de datos como de otros ámbitos, es necesaria para proporcionar criterios unificados y respuestas operativas sobre la aplicación de las reglas de protección de datos a los operadores globales, así como para poner en práctica estrategias conjuntas de garantía del cumplimiento de la norma.

3

E) IMPULSO DE LOS ENFOQUES PROACTIVOS: EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

La Agencia Española de Protección de Datos hace un seguimiento continuo de las novedades tecnológicas que impactan en la privacidad de las personas mediante un uso intensivo de sus datos personales. Por ello, y tal y como se ha mencionado con anterioridad, es consciente de la profunda transformación que se está produciendo en el ámbito del tratamiento de la información como consecuencia de la continua irrupción de nuevas tecnologías en un entorno social fuertemente marcado por la globalización y un cada vez mayor valor económico de los datos personales.

Por ello, de manera complementaria a los modelos tradicionales de supervisión –que continúan siendo completamente válidos– se hace necesario apostar por nuevos enfoques proactivos que tengan en cuenta los derechos de las personas desde las etapas iniciales del diseño de nuevos productos y servicios y que, además, fortalezcan la confianza de los ciudadanos mediante un compromiso responsable y una disposición diligente que evite o minimice los riesgos para la privacidad antes de que ocurran.

Para conseguir estos objetivos nació la metodología conocida como Protección de Datos desde el Diseño, que cuenta entre sus herramientas más útiles con las Evaluaciones de Impacto en la Protección de Datos Personales, desarrolladas fundamentalmente en países anglosajones pero perfectamente extrapolables a nuestro entorno y que cuentan ya con un importante grado de desarrollo y madurez.

Una Evaluación de Impacto en la Protección de Datos (EIPD) es un ejercicio de análisis de los riesgos que un sistema, producto o servicio puede implicar para la protección de datos y, tras haber realizado ese análisis, afrontar y gestionar esos peligros para eliminarlos o, al menos, mitigarlos en la medida de lo posible, antes de que se materialicen.

El objetivo es, por un lado, conseguir una tutela más activa del derecho fundamental a la protección de datos y, por otro, potenciar las políticas preventivas entre las organizaciones para evitar tanto costosos rediseños de los sistemas una vez han sido desarrollados como posibles daños a su reputación e imagen por un tratamiento inadecuado de los datos personales.

Por todo ello, la AEPD decidió promover estas nuevas herramientas en España mediante la publicación de una *Guía de Evaluación de Impacto en la Protección de Datos Personales*. Hay que resaltar que la versión definitiva se redactó tras difundir un primer borrador que fue sometido a consulta pública un periodo de seis semanas durante el cual, además de constatarse una acogida muy favorable a la misma (con una aceptación superior al 85%), se recibieron numerosas sugerencias muy útiles que fueron incorporadas a su versión definitiva.

En particular, la Guía indica situaciones en las que sería recomendable llevar a cabo este análisis. Entre ellas se pueden resaltar aquellos proyectos en los que se vayan a utilizar tecnologías que se consideran especialmente invasivas de la privacidad, como la videovigilancia a gran escala, el uso de drones, la minería de datos, el tratamiento de datos biométricos o genéticos, o la geolocalización.

También debería llevarse a cabo una EIPD cuando se realice un tratamiento con fines históricos, estadísticos o de investigación con datos no disociados; si el tratamiento está destinado a evaluar o predecir aspectos personales relevantes de los afectados como

su comportamiento o a encuadrarlos en perfiles determinados con cualquier finalidad; si está encaminado a tomar medidas que produzcan efectos jurídicos que afecten significativamente a las personas y, en particular, cuando establezcan diferencias de trato o trato discriminatorio; y si puede afectar a su dignidad o a su integridad personal.

Del mismo modo, se incluyen las situaciones en las que se traten grandes volúmenes de datos a través de herramientas como el Big Data, redes de contadores inteligentes (*smart grids)* o el Internet de las Cosas.

Es importante manifestar que la realización de las EIPD puede (y debe) integrarse dentro de las metodologías de análisis de riesgos y las listas de actividades de las herramientas de gestión de proyectos existentes en las organizaciones. El único requisito es que se tengan en cuenta los elementos esenciales de las EIPD y que se asegure que se ha realizado una revisión cuidadosa y sistemática del nuevo proyecto para identificar todos los posibles riesgos para la privacidad, haciéndose un esfuerzo serio por eliminarlos o reducirlos a un nivel aceptable y razonable.

Así, hay un conjunto de elementos comunes que forman parte del núcleo de cualquier procedimiento que se pueda considerar como una evaluación de impacto en el derecho fundamental a la protección de datos personales:

- Una EIPD es un proceso, más amplio que el de la mera comprobación del cumplimiento normativo y que debe llevarse a cabo con anterioridad a la implantación de un nuevo producto, servicio o sistema de información.

- Debe ser sistemático y reproducible, y estar orientado a revisar procesos más que a producir un resultado o informe final.

- Debe permitir una identificación clara de los responsables de las distintas tareas.

- Comienza con una primera fase de identificación y clasificación de la información para determinar los datos personales que se tratan y sus características.

- Debe identificar quién y cómo tendrá acceso y tratará los datos personales.

- Se debe permitir participar en el proceso y realizar aportaciones a todos los implicados en el mismo, tanto departamentos de la organización como socios o entidades externas, afectados u otros agentes sociales.

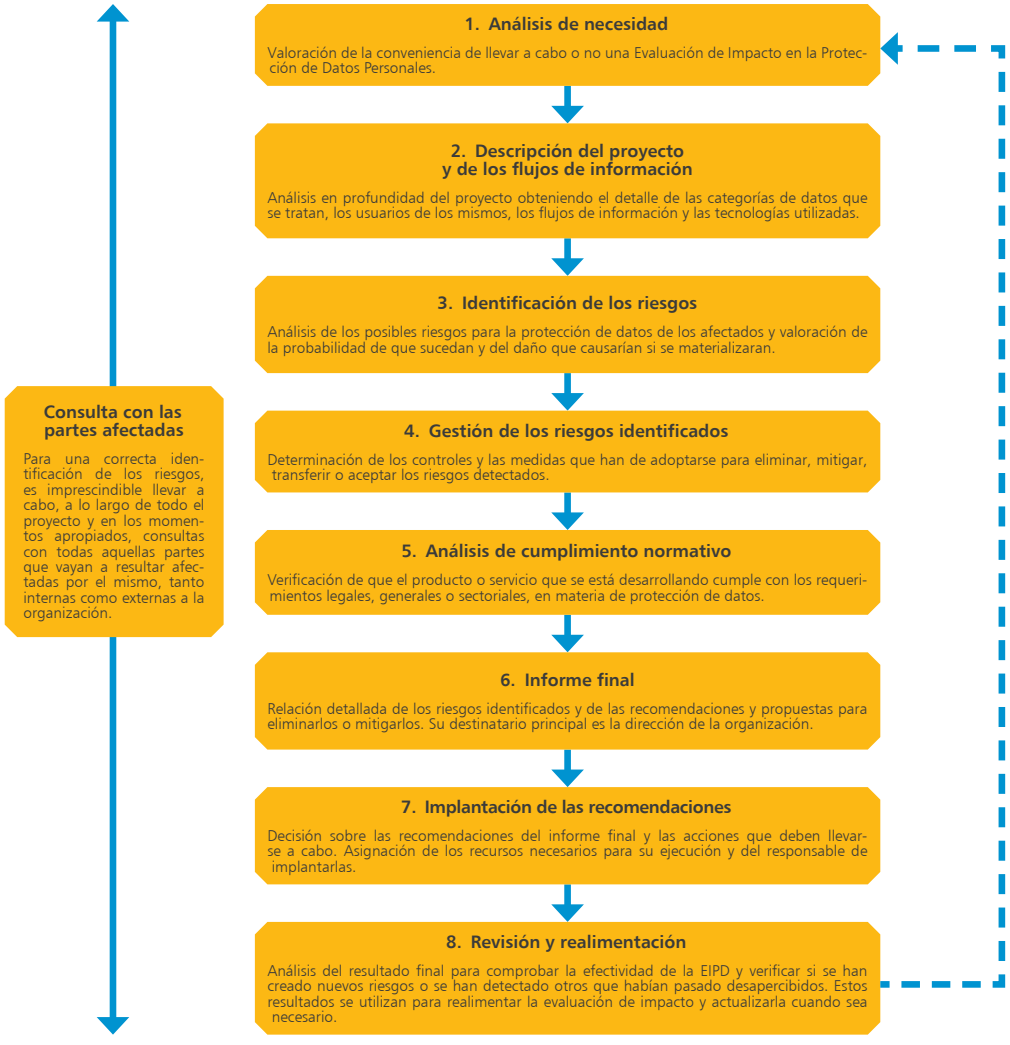
- Debe contener una descripción de los controles que se implantarán para asegurar que sólo se tratan los datos personales necesarios y para las finalidades legítimas previstas y definidas.

3

- El resultado final debe ser un documento con un contenido mínimo y una estructura que deben definirse previamente.

- El resultado final de un EIPD debería tener un cierto grado de publicidad en un documento distribuido por la organización que la ha realizado y que, por supuesto, no contendrá información confidencial o sensible.

Para garantizar que todos estos aspectos se recogen en la realización de una EIPD, la Guía detalla la necesidad de sistematizar el proceso en un conjunto de fases que garanticen la consecución de los objetivos de la evaluación, esto es, la correcta identificación y gestión de los riesgos para la privacidad. Estas fases se resumen en el siguiente gráfico:



<Índice>

Aunque en España no existe en estos momentos una obligación legal de realizar evaluaciones de impacto de esta naturaleza en ningún sector o ámbito específico, existen claros indicios de que esta situación va a cambiar y de que se va a acentuar claramente la importancia que van a tener estas metodologías en un futuro cercano.

Así, es necesario resaltar que tanto las previsiones de la Propuesta de Reglamento General de Protección de Datos para la Unión Europea como las recomendaciones de la Comisión Europea en ámbitos específicos como, por ejemplo, en el despliegue e instalación de las redes de contadores inteligentes, incluyen la necesidad de llevar a cabo evaluaciones de impacto en la protección de datos para detectar los riesgos por anticipado e implantar las necesarias medidas correctoras.

Además, el empleo de las evaluaciones de impacto mejorará sin duda las garantías para los derechos de las personas en aquellas organizaciones que las incorporen a sus sistemas y procedimientos de gestión de la privacidad, y contribuirá a generar más confianza en los usuarios y clientes de las mismas.

La realización de evaluaciones de impacto en las organizaciones, aunque no podrá ser considerada como un criterio de exención ante eventuales responsabilidades en caso de vulneración de la normativa de protección de datos, sí será tenida en cuenta por la AEPD como un elemento relevante para valorar si se ha adoptado la debida diligencia en la implementación de medidas para cumplir con las exigencias legales.

F) UNA POLÍTICA COORDINADA SOBRE EL USO DE APLICACIONES EN DISPOSITIVOS INTELIGENTES (APPS)

La Agencia Española de Protección de Datos participó en un análisis conjunto realizado por la Red Global de Control de la Privacidad (GPEN, Global Privacy Enforcement Network), en el cual se han estudiado los procedimientos utilizados por los desarrolladores de aplicaciones para garantizar la privacidad y la protección de los datos de usuarios de aplicaciones móviles. En particular, el análisis se centró en estudiar los procedimientos utilizados para informar al usuario de aplicaciones móviles sobre los tratamientos realizados así como los orientados a obtener su consentimiento para los posibles tratamientos de datos y para el acceso a la información almacenada en los dispositivos.

El informe fue realizado de forma conjunta por las autoridades competentes de diversos países, entre los que se encontraban Alemania, Canadá, España, Francia, Italia o Reino Unido, partiendo de una base de 1.200 aplicaciones seleccionadas de entre las más utilizadas por los usuarios en cada uno de los países en categorías como el ocio, la salud,

el ejercicio físico o la realización de transacciones bancarias, entre otras, e incluyendo versiones para dispositivos que utilizan los sistemas operativos iOS (Apple) y Android (Google).

El indicador primordial utilizado para el análisis fue el tipo de permisos solicitados por las aplicaciones y su adecuación a las necesidades reales del servicio prestado por la aplicación. El otro elemento central era la forma y manera en la que se informaba a los usuarios sobre las razones por las que se solicitaba acceso a su información personal y qué uso se le iba a dar a la misma.

Las Autoridades participantes en el análisis mostraron su preocupación por el hecho de que el 31% de las aplicaciones analizadas solicitaban permisos excesivos en relación a las funciones que presta la app. Los resultados del estudio ponen de manifiesto una situación ofrece un gran margen para la mejora de las garantías de los usuarios. Así, aunque podemos encontrar aplicaciones que se limitan a solicitar acceso a los datos que requieren para su funcionamiento normal, lo habitual es que las aplicaciones soliciten acceso a datos que no están relacionados con la funcionalidad que se ofrece, pero que pueden estar orientados a fines publicitarios con el fin de generar ingresos para el creador de la aplicación. Es un caso habitual en muchas de las aplicaciones de descarga gratuita de mayor difusión. También es habitual que aplicaciones recopilen información no relacionada en absoluto con su funcionalidad para obtener información que pueda ser ofrecida a terceros, usualmente con fines publicitarios.

El análisis de los datos consolidados mostró que en un 75% de los casos se solicitaba uno o más permisos de acceso al usuario, siendo los más habituales los referidos a los datos de ubicación, el identificador único del dispositivo, así como el acceso a otras cuentas de usuario gestionadas por el dispositivo, la cámara y los contactos del usuario.

En lo que se refiere a la información, en casi un 60% de los casos no resultaba fácil encontrar la relativa a los tratamientos de datos de carácter personal de forma previa a la instalación, presentando en muchos de ellos escasa o nula información, o remitiendo a sitios web en los que se ofrecía una política general sin elementos específicos adaptados a los tratamientos realizados por la aplicación móvil. Sólo en un porcentaje muy reducido de las aplicaciones se facilitaba información clara y suficiente al usuario, con una mayoría de aplicaciones proporcionando información insuficiente y un 30% que no ofrecía ninguna información más allá de la enumeración de los permisos de acceso que requería. En esa misma línea, poco más del 40% de las aplicaciones analizadas habían adaptado sus políticas de protección de datos para ser leídas en pantallas de reducidas dimensiones, obligando al usuario a navegar por políticas extensas sobre las que no resultaba fácil desplazarse, dificultando así que este obtuviera información adecuada.

El titular de los datos tiene derecho a recibir información clara y detallada sobre los tratamientos de datos que se van a realizar. En ese sentido, debe constar de forma clara que tipo de datos se van a recoger y tratar, con qué finalidad y de qué forma y ante quién puede el usuario ejercer sus derechos. Además, los usuarios de aplicaciones móviles tienen que considerar los beneficios de examinar con atención la información que se ofrece antes de instalar la aplicación, así como estar atentos a los permisos que se solicitan en el momento de instalarla. En caso de duda, siempre se puede tratar de obtener más información o tratar de encontrar otra aplicación que se ajuste mejor a las expectativas deseadas de privacidad.

<Índice>

Por lo que se refiere al proveedor del servicio, el estudio muestra que el ofrecer al usuario la información que necesita para poder decidir con conocimiento sobre el tratamiento de sus datos de carácter personal es un buen indicador del esfuerzo por parte del responsable de respetar los derechos de los individuos. Esto, sin considerar otros elementos igualmente importantes como la seguridad, es un signo positivo que el usuario ha de tener en cuenta a la hora de otorgar su confianza a un producto.

Por otro lado, y aunque la seguridad de las aplicaciones no formó parte del estudio, es de hecho uno de los elementos que preocupan a las Autoridades de protección de datos. En ese sentido, el responsable de la aplicación tiene la obligación de proporcionar un entorno seguro para el tratamiento de la información con medidas adecuadas al riesgo presente y a la naturaleza de los datos. No hay duda de que una seguridad adecuada redunda igualmente en una mayor confianza por parte de los usuarios.

En un último apunte sobre el carácter conjunto del análisis realizado, es evidente que el entorno globalizado en el que nos movemos en el ámbito de las telecomunicaciones impone la necesidad de cooperar en la resolución de los problemas derivados del uso de este tipo de tecnologías. Afortunadamente, y aun considerando las diferencias en los marcos legales de los países, la existencia de unos principios generales de protección de datos comúnmente reconocidos facilita la colaboración entre las Autoridades de distintos países. Aunque aún hay mucho camino por recorrer, iniciativas como la Red Global de Control de la Privacidad representan un paso adelante en esa dirección.

4 MARCOS SUPRANACIONALES DE PROTECCIÓN DE DATOS

A) AVANCE EN LA REVISIÓN DE LOS MARCOS INTERNACIONALES DE PROTECCIÓN DE DATOS

En 2014 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.

• Actualización del marco jurídico de la Unión Europea en materia de protección de datos

El 25 de enero de 2012 la Comisión Europea presentó dos propuestas de Reglamento General sobre Protección de Datos y de Directiva sobre protección de datos en el ámbito policial y judicial penal. A lo largo del año 2014 ha continuado el procedimiento legislativo ordinario en el que participan, de acuerdo con las previsiones del Tratado de Lisboa, el Consejo y el Parlamento Europeo.

El pleno del Parlamento Europeo confirmó el 12 de marzo de 2014 los informes sobre ambos textos adoptados por la Comisión LIBE en octubre de 2013. En este punto, hay que destacar que los textos aprobados por el Parlamento coinciden en gran medida con los presentados por la Comisión, si bien se introducen cambios que en su mayoría precisan y refuerzan el texto. Por otro lado, el Parlamento, a diferencia del Consejo, ha seguido en todo momento un enfoque integral en el análisis de las dos propuestas de la Comisión, respondiendo así al carácter unitario de la revisión que la propia Comisión ha defendido siempre.

En el Consejo, bajo las presidencias griega e italiana, la propuesta de Reglamento ha continuado debatiéndose en el seno del Grupo DAPIX. Ambas presidencias han mantenido un intenso ritmo de actividad lo que, probablemente unido a otros factores, ha conducido a que se hayan producido avances significativos en el desarrollo de las negociaciones.

En concreto, el Consejo de Justicia y Asuntos de Interior (JAI) ha aprobado tres Acuerdos Generales Parciales sobre otras tantas partes del Reglamento. Junto con la aplicación extraterritorial prevista en el artículo 3.2 de la propuesta de la Comisión, estos acuerdos se han producido sobre los capítulos dedicados a transferencias internacionales, obligaciones de responsables y encargados, y situaciones específicas de tratamientos, incluidas diversas modificaciones al artículo 1 del Reglamento introducidas con el fin de permitir una mayor flexibilidad a

los Estados miembros en los tratamientos realizados por los poderes públicos.

El valor de estos acuerdos sin embargo es limitado. Se aceptan bajo las condiciones de que «nada está acordado hasta que todo está acordado» y de que su aprobación no impide que las materias objeto de acuerdo vuelvan a reabrirse si así se hace necesario para conseguir coherencia con otras partes del documento. Estos acuerdos, además, no podrán servir en ningún caso como base para el inicio de trílogos informales con Parlamento y Comisión. Adicionalmente, varias delegaciones han presentado declaraciones sobre puntos específicos de algunos de estos capítulos. No obstante, y pese a estas cautelas, se han ido cerrando algunas de las partes más importantes del futuro Reglamento, al menos en términos de compromiso político.

El Grupo DAPIX volvió a discutir repetidamente sobre el sistema de ventanilla única, habiéndose logrado algunos avances sobre este punto. La Presidencia italiana reelaboró propuestas presentadas por Grecia, dando un mayor protagonismo en el proceso de toma de decisiones a las Autoridades de Protección de Datos distintas de la del establecimiento principal, en un intento de responder a las crecientes demandas de mayor proximidad al ciudadano. Este enfoque fue discutido en el último Consejo JAI bajo Presidencia italiana celebrado el mes de diciembre y obtuvo un apoyo mayoritario a sus elementos estructurales, si bien la adopción de un acuerdo general parcial, quedó pendiente de ulteriores trabajos del Grupo en un nivel técnico.

Las negociaciones sobre la Directiva han seguido un ritmo más pausado, con un número mucho menor de reuniones y unos resultados también más limitados. Por el momento se continúa la segunda revisión del texto, sin que se haya remitido al Consejo JAI ningún tipo de propuesta concreta.

El procedimiento legislativo está, por tanto, pendiente de que el Consejo adopte su posición común. Existen fuertes presiones políticas para conseguir una pronta adopción de estos instrumentos, especialmente del Reglamento. Tanto la Comisión designada en 2014 como el Consejo Europeo han fijado como objetivo la aprobación definitiva del texto en 2015. Letonia, que ostenta la presidencia durante el primer semestre de 2015, anunció antes de iniciar su mandato su intención de finalizar las discusiones del Reglamento en el Consejo en junio de 2015.

Como ya se ha indicado en anteriores memorias, la AEPD, 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. No obstante, ha seguido, aún más intensamente en atención a los temas tratados, prestando asesoramiento y asistencia a los departamentos responsables en el marco de los mecanismos de coordinación que se han establecido para la tramitación de este paquete normativo.

Junto con esa labor de cooperación, la AEPD ha participado también activamente en la preparación de las reacciones de las Autoridades de protección de datos de los Estados miembros de la UE, reunidas en el Grupo de Trabajo del Artículo 29 (GT29), a estas iniciativas normativas. Además de en las Opiniones ya mencionadas en anteriores memorias, ha tenido un papel relevante en la elaboración de las posiciones que se citan posteriormente, en particular en la referida a la «ventanilla única», en la que la AEPD actuó como co-redactor.

- **Actualización del Convenio 108 del Consejo de Europa**

Aunque su impacto directo en el derecho español de protección de datos sea aparentemente menor, no puede obviarse la importancia del segundo de los instrumentos europeos actualmente en proceso

de revisión. Se trata del Convenio 108 del Consejo de Europa, cuya reforma se abordó al 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, en noviembre de 2012, remitió al Comité de Ministros la propuesta definitiva de texto articulado.

Posteriormente, y a lo largo de 2013 y 2014, un comité *ad hoc* (CAHDATA), en el que está presente la Presidencia del Comité Consultivo, ha estudiado el texto siguiendo el mandato, que incluye plazos, que emite el Comité de Ministros a propuesta del Standing Committee on Media and Information Society. El CAHDATA ha celebrado un total de tres reuniones y tras la última elevó una propuesta de texto al Comité de Ministros.

Como ya se destacó en memorias anteriores, un elemento clave en este proceso de revisión es que la Unión Europea ha reivindicado formalmente que su competencia en materia de protección de datos debe extenderse a la negociación y adopción de la nueva Convención. Para ello, el Consejo otorgó un mandato de negociación a la Comisión, que ha participado en las reuniones del CAHDATA. Si bien en algunas de las materias cubiertas por el Convenio los Estados miembros siguen manteniendo sus competencias, en una parte sustancial de su ámbito de aplicación, la Comisión sustituye a los Estados miembros que, en su caso, y dependiendo de cómo se resuelva finalmente la cuestión aún abierta de los derechos de voto de la Unión Europea, estarían obligados a refrendar con sus votos las posiciones defendidas por la Comisión.

B) LA ACTIVIDAD DEL GRUPO DE TRABAJO DEL ARTÍCULO 29

Durante el año 2014 las Autoridades de protección de datos de los Estados miembros de la UE, reunidas en el Grupo de Trabajo del artículo 29 (GT29), han celebrado cinco reuniones plenarias en las que se han adoptado nueve dictámenes y tres documentos de trabajo. También se han acordado y remitido varias cartas que reflejan la posición del Grupo en temas de relevancia actual, incluida una sobre «ventanilla única». Especial mención merece, además, la aprobación de un documento que establece criterios comunes de interpretación y aplicación de la Sentencia del Tribunal de Justicia de la UE en el caso Google Spain e Inc. vs. AEPD y Mario Costeja González. Asimismo, se ha continuado con la actuación coordinada e iniciada en años anteriores en relación con la nueva política de privacidad de Google, de la que se informa posteriormente.

A continuación, se describen los documentos de mayor interés aprobados en el seno del GT29[1]:

- **Propuesta de reforma de la normativa de protección de datos**

El GT29 ha elaborado varios documentos sobre la revisión del marco normativo europeo desde el inicio del procedimiento legislativo en 2012. Lógicamente, la prolongación en el tiempo del proceso ha hecho que la actividad del Grupo también haya perdido intensidad, a la espera de que se conozcan las posiciones de partida de los colegisladores europeos.

En 2014 el GT29 ha adoptado un documento de especial relevancia que avanza en la definición de su posición en un tema tan crítico en el contexto de la reforma como es el de la «ventanilla única».

[1] Una relación completa de los mismos puede consultarse en la página web del GT29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm)

<Índice>

El Grupo ya había establecido anteriormente determinados elementos básicos en su valoración del *one stop shop*. La Declaración aprobada en 2014, que se adjuntaba como anexo a una carta enviada a la Presidencia griega del Consejo y al presidente de la Comisión LIBE del Parlamento, considera que un sistema de ventanilla única válido tanto para empresas como para los ciudadanos debería basarse en los siguientes puntos:

- Todas las Autoridades de protección de datos (APD) son competentes para supervisar la aplicación del Reglamento en sus respectivos Estados, incluido cuando los residentes en el territorio de ese Estado están afectados por el tratamiento.
- Las decisiones sobre los casos transnacionales de menor entidad o los puramente nacionales deben ser tomadas por las APD nacionales afectadas.
- Si la APD líder (del estado donde se sitúa el establecimiento principal del responsable o encargado) y las APD nacionales están de acuerdo en la solución de un caso, la APD líder tomará todas las medidas relevantes respecto del establecimiento principal.
- Excepcionalmente, si no alcanzan un acuerdo, el asunto será tratado por el Consejo Europeo de Protección de Datos.
- Las decisiones de una APD que se refieran a personas cuya queja haya sido rechazada deberían poder ser recurridas ante los tribunales del Estado miembro donde se ha presentado la queja.
- El Consejo Europeo de Protección de Datos debería ser reforzado para emitir directrices vinculantes u otro tipo de medidas cuando las APD afectadas en casos transfronterizos no alcancen un consenso.

- **Dictamen sobre la aplicación de los conceptos de necesidad y proporcionalidad, y la protección de datos en el sector de los organismos con funciones coercitivas *(law enforcement)* (WP 211)**

Este Dictamen ha sido elaborado con el objetivo de destacar la importancia de la correcta consideración de los conceptos de necesidad y proporcionalidad a la hora de diseñar medidas en el ámbito policial y judicial penal (*law enforcement*) que requieran el tratamiento intensivo de datos de carácter personal. Si bien los conceptos trascienden del contexto más general de privacidad, resulta importante entender su relación con la protección de datos a la luz del análisis de la jurisprudencia sobre la materia tanto del Tribunal Europeo de Derechos Humanos como del Tribunal de Justicia de la UE.

En el análisis de estas medidas, y de acuerdo al Dictamen, se han de tener en consideración los siguientes elementos:

- La necesidad de una base jurídica clara.
- La persecución de uno de los objetivos legítimos establecidos en el artículo 8.2 de la Carta Europea de los Derechos Humanos:
  - Necesaria en una sociedad democrática:
    - Existencia de una necesidad social imperiosa.
    - Determinar la gravedad del problema.
    - Tener en cuenta las actitudes individuales, rasgos culturales y el margen de aplicación de la norma.
  - Proporcional:
    - Objetivos claros y finalidades específicas.
    - Revisar tanto las medidas existentes en el mismo ámbito como las diferentes alterna-

tivas, en especial aquellas que sean menos intrusivas.

– Garantizar la adecuación de las medidas y evitar los excesos.

– Determinar el periodo de conservación de los datos.

– Aplicar un enfoque holístico teniendo en cuenta cómo la medida propuesta complementa a las ya existentes y, si todas ellas en su conjunto mantienen la necesaria proporcionalidad del sistema.

- Motivos pertinentes y suficientes, basando las propuestas en evidencias contrastables.

En el ánimo del Grupo de Trabajo está ayudar con este Dictamen a los legisladores y a las Autoridades con funciones de cumplimiento de la ley para un mejor entendimiento de los elementos que hay que tener en cuenta para evitar que cualquier medida en este ámbito que se adopte en el futuro se limite a aportar «valor añadido» o a «ser útil», en vez de ser necesaria y proporcionada, además de favorecer el cumplimiento de los principios aplicables a la protección de datos de carácter personal.

- **Dictamen (WP 215) y Documento de Trabajo (WP 228) sobre vigilancia de comunicaciones electrónicas para finalidades de inteligencia y seguridad nacional**

Desde el verano de 2013 los medios de comunicación se hicieron eco de las actividades de vigilancia llevadas a cabo por servicios de inteligencia tanto de Estados Unidos como europeos a partir de las revelaciones de Edward Snowden.

El GT29 reaccionó desde un primer momento a estas informaciones en la forma en que ya se ha indicado en anteriores memorias. En la correspondiente a 2013 se anunciaba, además, que el Grupo estaba preparando un Dictamen sobre estos temas.

Este Dictamen ha sido adoptado en 2014 y parte de la constatación de que la privacidad y la protección de datos son derechos fundamentales reconocidos por instrumentos internacionales universales y europeos. De ello se deduce que el respeto al marco jurídico europeo e internacional implica que estos derechos reciban el más alto nivel de protección.

El Grupo concluye en su análisis que los programas de vigilancia secreta, masiva e indiscriminada son incompatibles con nuestras leyes fundamentales y no pueden ser justificados por razones de lucha contra el terrorismo o contra otras importantes amenazas a la seguridad nacional. Las restricciones a los derechos fundamentales sólo son aceptables si son estrictamente necesarias y proporcionadas en una sociedad democrática.

Por todo ello, el GT29 recomienda varias medidas para asegurar que el imperio de la ley es respetado y asegurado. Entre ellas pueden citarse:

- Mayor transparencia sobre cómo operan estos programas y sobre lo que las autoridades encargadas de su supervisión hacen y deciden.
- Más transparencia por parte de los responsables a los que se dirigen las peticiones de acceso de los servicios de inteligencia.
- Necesidad de mayor sensibilización de los ciudadanos.
- Establecimiento de un sistema legal coherente para los servicios de inteligencia, que incluya disposiciones sobre protección de datos.
- Asegurar una supervisión eficaz de la actividad de los servicios de inteligencia.

<Índice>

- Asegurar que los responsables sujetos al derecho de protección de datos europeo cumplen con sus obligaciones.

El Dictamen se apoyaba en un análisis jurídico de los diversos elementos y conceptos involucrados en el contexto de los programas de vigilancia masiva. Dada la extensión de este análisis, se optó por emitir el Dictamen de recomendaciones y hacer una publicación posterior, separada, de los trabajos de preparación. Esos trabajos constituyen el contenido del Documento de Trabajo WP 228.

En esta misma línea de reacción a las informaciones sobre los programas de vigilancia masiva de los ciudadanos europeos, el GT29 dirigió a la entonces vicepresidenta de la Comisión Europea, Viviane Reding, una carta para transmitirle una serie de recomendaciones adicionales a incluir en las negociaciones que la Comisión Europea viene manteniendo con las autoridades norteamericanas para reformar el Safe Harbor.

Como se ha indicado, uno de los elementos de los programas de vigilancia era el acceso a datos transmitidos desde la UE a EEUU por compañías norteamericanas y la Comisión, en una comunicación de noviembre de 2013, ya anunció que se abrirían negociaciones para mejorar el funcionamiento de este sistema y resolver sus principales debilidades. Esta comunicación fue, además, acompañada por un informe específicamente dedicado a evaluar el actual modelo de Safe Harbor. Hay que recordar que el Safe Harbor es un sistema de adecuación sectorial, por el que se aprueba que las empresas que se auto-certifican como cumplidoras de los principios del Safe Harbor puedan recibir datos desde la UE sin ningún tipo de restricción o requisito previo. Aunque la decisión es adoptada unilateralmente por las instituciones de la Unión, la Comisión puede entablar negociaciones con el país afectado a fin de evaluar si las garantías que éste ofrece suponen el «nivel adecuado de protección» que exige la Directiva.

En la carta y en el anexo, el GT29 muestra su apoyo a las medidas de reforma previstas por la Comisión en su informe y propone medidas adicionales en materias como ley aplicable, transparencia, recursos, acceso de las autoridades americanas, costes para los interesados, etc. Aunque la Comisión anunció que las negociaciones para la revisión de la decisión de Safe Harbor finalizarían en el verano de 2014, al finalizar el año referente a esta Memoria no se habían concluido aún las discusiones con la parte norteamericana.

- **Dictamen sobre técnicas de anonimización (WP 216)**

En este Dictamen se analiza la eficacia y las limitaciones de las técnicas de anonimización existentes en la actualidad, atendiendo al marco legal de la UE sobre protección de datos y formulando una serie de recomendaciones para la gestión de estas técnicas.

La conclusión fundamental del texto es que las técnicas de anonimización, si bien contribuyen a aportar garantías de privacidad, necesitan que su aplicación se base en un diseño adecuado, lo que implica que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada, manteniendo la utilidad de los datos en el contexto en el que quieren ser utilizados. Es fundamental tener en cuenta el riesgo residual de identificación inherente a cada técnica como consecuencia del avance de las técnicas de reidentificación, así como la existencia de fuentes alternativas de información que pueden ser utilizadas como vía indirecta para obtener la identidad, o al menos singularizar a los individuos afectados. La solución óptima ha de decidirse caso por caso y tras un análisis cuidadoso, pudiendo conllevar la utilización conjunta de diversas técnicas con ese fin.

El documento presta especial atención al concepto y a las técnicas de seudonimización, tratando de incidir sobre algunos errores e ideas falsas asociados a este concepto. La seudonimización *per se* no es un método de anonimización que garantice la disociación de la información respecto de la identidad subyacente. Simplemente reduce el grado de vinculación de un conjunto de datos con la identidad original del individuo y, en consecuencia, no cabe ser considerado sino como una medida de seguridad útil. En todo caso, los responsables del tratamiento deben ser conscientes de que un conjunto de datos, aún disociado, puede entrañar todavía riesgos residuales para los interesados.

- **Dictamen sobre la noción de intereses legítimos del responsable en relación al artículo 7.f) de la Directiva 95/46 (WP 217)**

Este Dictamen es el último de una serie de documentos adoptados por el GT29 respecto a disposiciones clave de la vigente Directiva y ha ido precedido de otros como los relativos a la noción de dato personal, el consentimiento o el principio de limitación de finalidad.

El documento parte de la constatación de que el artículo 7.f) de la Directiva ha sido transpuesto y aplicado de formas muy variadas en los Estados miembros. Esta diversa interpretación del artículo conduce a que en algunos Estados miembros esta base legal de los tratamientos se utilice sólo como último recurso y en situaciones ciertamente especiales, mientras que en otros, por el contrario, es la base legitimadora de preferencia al considerarse que resulta menos exigente que las demás que contiene el artículo 7 de la Directiva.

El GT29 sostiene que el interés legítimo del responsable es una más de las bases legales que la Directiva ofrece y que adecuadamente empleada puede no sólo ofrecer espacios adicionales para el tratamiento de datos personales sino, sobre todo, evitar un uso inapropiado, cuando no un abuso, de otras bases legales.

El Dictamen analiza el interés legítimo y sus relaciones con las demás bases del artículo 7 y posteriormente estudia los principales conceptos de esta disposición, señaladamente el de «intereses legítimos del responsable» (o de los terceros a los que se cedan los datos) y los de intereses, derechos o libertades fundamentales de los interesados.

La parte central del documento es la que se refiere al análisis de la ponderación que requiere la utilización del interés legítimo. Se trata de la única base legal que exige este tipo de ejercicio, ya que es la única en que junto con el criterio de que el tratamiento ha de ser necesario para satisfacer un determinado interés, en este caso un interés legítimo del responsable, es preciso evaluar si los intereses, derechos o libertades de los usuarios no prevalecen sobre tal interés legítimo.

El Dictamen contiene también una *Guía rápida* en la que se detalla de forma sistemática, ordenada y resumida los pasos que deben darse para llevar a cabo esa ponderación, así como un anexo con un gran número de ejemplos que pretenden no tanto ofrecer una serie de respuestas correctas a determinados supuestos donde el interés legítimo podría ser aplicable como ilustrar la lógica del proceso de ponderación y la importancia de todos sus elementos.

- **Dictamen sobre aplicación de la Directiva 2002/58/CE al seguimiento de la huella de dispositivos *(device fingerprinting)* (WP 224)**

Este Dictamen parte de la constatación de que el seguimiento que puede realizarse de las huellas que dejan los dispositivos utilizados para navegar por internet puede afectar seriamente a la protección de datos de los ciudadanos. De hecho, varios

<Índice>

servicios online han propuesto este tipo de seguimiento como una alternativa a las conocidas cookies a efectos de analizar la navegación o hacer un seguimiento de los usuarios sin necesidad de obtener el consentimiento que prevé el artículo 5.3 de la Directiva 2002/58.

El mensaje central del Dictamen es que este artículo se aplica al *device fingerprinting* e indica a los terceros (distintos del editor de la web en que se navega) que traten la huella que los dispositivos generan cuando se accede a, o se almacena información en el dispositivo terminal del usuario, que sólo pueden hacerlo con el consentimiento de éste salvo que sean de aplicación algunas de las excepciones contempladas en la propia Directiva. En este sentido, el Dictamen es una ampliación de otro anterior, el 4/2010, sobre excepciones al consentimiento en el uso de cookies.

- **Documento de trabajo sobre Borrador de cláusulas contractuales ad hoc de «encargado en UE para subencargado no en UE» (WP 214)**

Este Documento de Trabajo (1/2014) es una revisión de las cláusulas contractuales para transferencias de responsable a encargado del tratamiento contenidas en la Decisión 2010/87 de la Comisión.

Esas cláusulas son el resultado de una revisión de la versión original dirigida a facilitar la subcontratación por parte de los primeros encargados. El problema es que, dado que los flujos de datos internos en la Unión Europea no tienen la consideración de transferencias internacionales en sentido estricto y no están sometidos a ningún tipo de control o autorización, la aplicabilidad de estas cláusulas se limita a los casos en que el primer encargado es una empresa de países terceros y no procede cuando el primer encargado es una empresa europea.

La Agencia Española fue la primera en intentar hacer frente a la situación de relativa desventaja en que quedan las empresas europeas, que no pueden beneficiarse de la mayor flexibilidad que permiten las cláusulas cuando actúan como encargados y subcontratatistas entidades fuera de la Unión. Para ello, desarrolló un modelo de cláusulas *ad hoc* que se basaban en las cláusulas estándar de 2010 pero añadiendo una serie de precisiones para permitir su aplicación a la actividad de subcontratación por los encargados europeos.

Partiendo de las cláusulas desarrolladas por la Agencia, el GT29 ha elaborado su propio modelo de cláusulas *ad hoc*, introduciendo modificaciones que supriman o reduzcan los obstáculos que plantean tanto las cláusulas originales como la adaptación hecha por la AEPD, lógicamente ajustada a nuestro ordenamiento jurídico.

Las cláusulas contractuales contenidas en este Documento no han sido formalmente adoptadas por la Comisión y, por tanto, no constituyen un nuevo modelo oficial de cláusulas estándar. Por ello, tampoco puede entenderse que su utilización suponga automáticamente que se estén ofreciendo las

garantías suficientes previstas por la Directiva. El propósito del Documento es ofrecer a la Comisión un material que pueda utilizar si en el futuro decide aprobar unas cláusulas modelo de este tipo y, al mismo tiempo, facilitar una aplicación uniforme de las autorizaciones de las transferencias de datos personales en los ámbitos nacionales.

En definitiva, si bien éstas no son cláusulas tipo cuyo uso exima de solicitar autorización en algunos Estados miembros, el hecho de que sean utilizadas por las empresas permitiría procesos de autorización muy mecánicos y con resultados comunes en toda la UE.

- **Declaración sobre el papel del enfoque de riesgo *(risk based approach)* en los marcos legales de protección de datos (WP 218)**

Esta Declaración es la respuesta del GT29 a las iniciativas que vienen proliferando desde hace cierto tiempo y que tienen como objetivo promover la implantación del llamado «enfoque de riesgo» en al ámbito de la protección de datos.

La noción de enfoque de riesgo no es nueva en el contexto de la protección de datos de carácter personal. La Directiva 95/46 contiene varias disposiciones en que una obligación o unas medidas pueden o deben ser moduladas según los riesgos que el tratamiento conlleve.

Sin embargo, estas nuevas propuestas, originadas fundamentalmente en entornos empresariales, parecen trasladar el foco de esta orientación desde el terreno de las obligaciones al de la legitimación de los tratamientos, convirtiendo el enfoque de riesgo en una alternativa a los tradicionales principios y derechos de protección de datos.

La Declaración recuerda que la protección de datos es un derecho fundamental y que cualquier operación de tratamiento, desde la recogida hasta la destrucción o cesión debe respetar este derecho. Los interesados deben mantener sus derechos con independencia del nivel de riesgo que pueda conllevar el tratamiento, y los principios fundamentales aplicables a los responsables (legitimación, minimización, finalidad o transparencia, entre otros) deberían continuar siendo los mismos sea cual sea el tipo de tratamiento o los riesgos para los interesados.

La implementación de las obligaciones de los responsables a través de las medidas de *accountability*, no obstante, puede y debe variar en función del tipo de tratamiento y de los riesgos para los interesados. En este sentido, el documento señala que los riesgos deben valorarse a partir de criterios objetivos, que esos riesgos deben referirse a los derechos y libertades fundamentales de los interesados, incluido el derecho a la protección de datos, y que el concepto de riesgo debe entenderse de una manera más amplia que el de mero daño.

- **Actuación coordinada en relación con la nueva política de privacidad de Google**

El procedimiento coordinado que las Autoridades europeas de protección de datos iniciaron en febrero de 2012 en relación con la nueva política de privacidad de Google se ha extendido también a 2014.

Por una parte, varias de las Autoridades de protección de datos que habían iniciado procedimientos sancionadores contra Google y que se integran en el grupo de trabajo que se formó en 2013 siguiendo las sugerencias del GT29 (Alemania –Hamburgo–, España, Francia, Holanda, Italia y Reino Unido) los han continuado y cerrado a lo largo del año. Esta es la situación de Francia, Holanda, Alemania

<Índice>

e Italia. En todos estos casos, así como en el de la resolución ya adoptada por la AEPD en 2013, y aunque los contenidos concretos varían en función de los distintos marcos legales, las decisiones coinciden tanto en establecer que Google ha vulnerado las respectivas leyes de protección de datos como en que esas vulneraciones afectan a la capacidad de los ciudadanos de saber qué se hace con sus datos personales y de ejercer un control eficaz sobre ellos. Asimismo, en todas estas decisiones se incluyen medidas sancionadoras de diferentes tipos y requerimientos a la compañía para revisar su política de privacidad.

Por otro lado, Google ha generalizado sus contactos a lo largo del año con todas las Autoridades integrantes del Grupo de Trabajo y ha continuado los que mantenía con este en su conjunto, al tiempo que ha remitido a estas Autoridades sucesivas propuestas de modificaciones que ofrece introducir, o ya ha introducido, tanto en su política de privacidad como en los mecanismos de información y de control por parte de los usuarios.

El GT29, por su parte, acordó en su reunión plenaria del mes de junio que prepararía un conjunto de recomendaciones dirigidas a Google con el fin de precisar las ya formuladas en la carta remitida a la compañía en octubre de 2012. Estas recomendaciones estarían basadas principalmente en los elementos que son comunes a las resoluciones ya adoptadas o pendientes de adoptar por las Autoridades integradas en el grupo de trabajo y enriquecidas por las aportaciones de otras Autoridades del GT29.

Según lo previsto, las recomendaciones fueron aprobadas en el plenario del mes de septiembre y se comunicaron mediante una carta a Google. Estas medidas son indicativas y pretenden tan solo servir de guía para la compañía, sin que impidan la implantación de otras opciones alternativas siempre que se obtengan los mismos resultados en términos de cumplimiento.

C) ÁREA DE COOPERACIÓN POLICIAL Y JUDICIAL

• Sistema de información Schengen

A lo largo del año se ha ido consolidando la estructura de supervisión del Sistema de Información Schengen de segunda generación. El Grupo de Supervisión Coordinada SIS II (GSC SIS II) ha establecido su programa de trabajo, comenzando en primer lugar por cerrar las tareas pendientes de la extinta Autoridad de Control Schengen, en particular un ambicioso estudio sobre el ejercicio del derecho de acceso que ha sido publicado a finales de 2014.

Respecto a la investigación de la quiebra de seguridad que afectó a la copia nacional del SIS de primera generación de Dinamarca en el año 2012, finalizaron los trabajos del grupo creado por la Comisión Europea, dándose a conocer un conjunto de recomendaciones de carácter específico y de aplicación tanto a nivel de sistema central como de las unidades nacionales que van a permitir, de llevarse a cabo su implementación, ayudar mitigar los riesgos de seguridad del sistema y a manejar de forma más eficaz cualquier posible incidente. No obstante, siguen sin conocerse con detalle los elementos técnicos y de procedimiento, incluyendo la existencia de vulnerabilidades en el sistema, que pudieron haber facilitado el acceso a dicha información por parte de terceros.

En otro orden de cosas, tras el cambio en el sistema de evaluación Schengen, que desplaza la responsabilidad de la organización de las auditorías a la Comisión Europea en colaboración con los Estados miembros, se han desarrollado los cuestiona-

rios de evaluación que van a ser utilizados como medio de preparación de las auditorías así como los procedimientos de selección del personal evaluador a propuesta de los Estados miembros y con la participación de la Comisión Europea. De esta forma, y de acuerdo a lo establecido en el Reglamento 1053/2013, por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen, los equipos evaluadores pasan a estar conformados por representantes de los Estados miembros –previa selección en base a su cualificación–, representantes de la Comisión Europea y observadores de organismos de la Unión implicados en la aplicación de Schengen, como Frontex o Europol.

Las primeras evaluaciones con el nuevo sistema tendrán lugar en el primer semestre de 2015, comenzando por Austria, Bélgica y Polonia.

Tras el resultado favorable del procedimiento de evaluación pre-acceso realizada al Reino Unido, en el que participó la AEPD, el Reino Unido formalizó su deseo de unirse al SIS II a partir de octubre de 2014. Razones derivadas del derecho de salida (*opt out*) de las medidas de cooperación policial y judicial ejercido por el Reino Unido con efectos desde el 1 de diciembre de 2014 –aunque ha manifestado su voluntad de permanecer en un conjunto de ellas, incluyendo la integración en el SIS II– y las reticencias de algunos de los Estados miembros, basadas tanto en razones técnicas como jurídicas, han conducido a un retraso de la integración efectiva.

- **Oficina de Policía Europea, Europol**

El año 2014 ha visto avanzar la tramitación de la propuesta de nuevo Reglamento Europol tanto en el Parlamento Europeo –que aprobó su primera lectura– como en el Consejo, que aprobó una posición común sobre la misma poniendo particular énfasis en el debate sobre las disposiciones que afectan a la protección de datos de datos de carácter personal.

La Autoridad Conjunta de Control de Europol ha manifestado su opinión sobre la propuesta en tres documentos. El primero fue publicado en junio y el segundo, con un análisis de detalle de la propuesta, en octubre de 2013. El tercero, centrado en aspectos específicos, fue dado a conocer a finales de 2014. El GT29 no ha elaborado una opinión formal y se ha limitado a enviar una carta tanto al Parlamento como al Consejo Europeo, indicando los criterios a tener en cuenta en la configuración del modelo de supervisión en Europol.

La Agencia ha venido asesorando tanto al Ministerio del Interior –a través de la Dirección General de la Policía– como a la Representación Permanente de España en Bruselas en aspectos técnicos relacionados con la tramitación de este Reglamento. A finales de 2014 comenzaron los contactos entre el Parlamento, el Consejo y la Comisión en busca de un texto común que se espera sea aprobado a mediados de 2015.

Un debate particularmente interesante ha sido el relativo al modelo a seguir en el ámbito de la supervisión de la protección de datos. Tanto la propuesta de la Comisión como el resultado de la primera lectura en el Parlamento Europeo otorgan un papel predominante al Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés) en detrimento de una participación más activa de las autoridades de los Estados miembros. Por su parte, el Consejo ha optado por, manteniendo la posición relevante del EDPS, dar un papel de peso a los mecanismos de supervisión coordinada con las autoridades de los Estados. Esta discusión se trasladará, sin duda, a las negociaciones a tres.

<Índice>

En el marco de las actividades de supervisión realizadas por la Autoridad Común de Control, la Agencia Española de Protección de Datos ha participado en la auditoría anual que tuvo lugar en el mes de marzo en la sede central de Europol en La Haya. Como resultado de dicha auditoría, se ha formulado un conjunto de recomendaciones técnicas y de procedimiento que Europol ha de implantar de acuerdo al plan de acción diseñado en cooperación con la Autoridad Común de Control. En ese sentido, hay que señalar la importancia adquirida a lo largo de los años por las auditorías anuales como elemento central en el proceso que ha permitido a Europol mantener un alto nivel de protección de datos de carácter personal.

Por último, resaltar también la tarea de los subgrupos incluidos en la estructura de la Autoridad Común de Control, en particular el subgrupo de nuevos proyectos, en el que participa la Agencia, y que es el encargado de examinar, de forma conjunta con Europol, los elementos técnicos y de procedimiento a la hora de asegurar que cualquier desarrollo puesto en marcha por Europol mantiene un estándar elevado en lo tocante a seguridad y protección de datos.

- **Sistema de Información de Visados**

El Sistema de Información de Visados continúa su despliegue de acuerdo a la planificación por zonas diseñada por la Comisión Europea.

En mayo de 2014 se completó el despliegue en las regiones 12.ª a 15.ª[2], y en septiembre de 2014 se puso en marcha en la 16.ª región, que incluye a Albania, Antigua República Yugoslava de Macedonia, Bosnia y Herzegovina, Kosovo Montenegro, Serbia y Turquía. Se está trabajando en el despliegue del sistema en Rusia y Ucrania –incluidas en las regiones 17.ª y 18.ª–, tras lo cual se espera completar el despliegue en el sur y este de Asia, incluyendo China, la India, Pakistán y Bangladesh, finalizando con Andorra, el Vaticano, Mónaco, San Marino, Irlanda y el Reino Unido.

Las actividades de supervisión conjunta se están centrando en estos momentos en el análisis de las Autoridades nacionales con acceso al sistema, el acceso al sistema con fines de cumplimiento de la ley y la posibilidad del ejercicio de los derechos reconocidos a los afectados. De la misma forma, se trabaja en el análisis de las actividades de las empresas que actúan como agentes de las representaciones diplomáticas en el extranjero y que se ocupan de la recogida de la documentación así como en un marco de supervisión conjunto, incluyendo la posibilidad de inspecciones conjuntas en países donde una misma empresa se encargue de la solicitudes de visado correspondientes a varios Estados miembros. Por último, es materia de investigación la calidad de los datos transmitidos al sistema central por parte de los Estados miembros, en particular la calidad y presencia de los datos biométricos.

En la línea de esos objetivos, se han desarrollado un grupo de cuestionarios que faciliten el análisis previo de estas cuestiones. A estos cuestionarios podrán seguir actividades –en el ámbito nacional o en forma de actuaciones conjuntas– con participación de las Autoridades de varios Estados miembros, en particular en lo relacionado con el uso de empresas externas para la tramitación inicial de las solicitudes de visado.

En su última reunión de 2014, el Grupo de Supervisión Coordinada –formado por las Autoridades nacionales de supervisión y el EDPS– decidió crear un grupo de trabajo que se ocupe de la elaboración de una propuesta de sistema de auditoría con el

[2] Estas regiones incluyen países de América del Norte y Central, así como de la cuenca del Pacífico.

fin de facilitar a los Estados miembros y a las Autoridades de protección de datos el cumplimiento de las obligaciones que, en ese sentido, establece el Reglamento sobre el Sistema de Información de Visados. Conviene recordar que obligaciones similares se han recogido en las normas que regulan el funcionamiento del Sistema de Información Schengen de segunda generación (SIS II), por lo que es factible aprovechar las sinergias que se puedan derivar del trabajo realizado por el Grupo de Supervisión Coordinada del VIS.

- **Eurojust**

La Comisión presentó la propuesta de Reglamento sobre Eurojust el 17 de julio de 2013. El grupo de trabajo del Consejo responsable de esta propuesta ha venido desarrollando las discusiones sobre la misma durante las presidencias lituana y griega, aunque el debate ha alcanzado su punto álgido durante la italiana.

Sin perjuicio de la evolución de la negociación de la propuesta de Reglamento de Europol, por su incidencia indirecta en esta negociación, han sido objeto de discusión las consecuencias de la adopción de un régimen de protección de datos basado en la aplicabilidad directa del Reglamento 45/2001 y supervisión por el EDPS sobre el normal funcionamiento de Eurojust. Tanto la Comisión como el EDPS apoyan dicha postura sobre la base jurídica de la necesaria adaptación de todas las Agencias europeas a su supervisión una vez transcurridos cinco años desde la vigencia del Tratado de Lisboa. El Servicio Jurídico del Consejo ha afirmado que ello no tiene que ser necesariamente así y que es posible en su opinión un régimen específico de protección de datos e incluso cabría un regulador diferente al EDPS siempre que se cumplan los requisitos precisos para ello de acuerdo con la doctrina judicial del TJUE en los casos C-518/07, Comisión Europea contra República Federal de Alemania y C-614/10, Comisión Europea contra Austria entre otros, que implican independencia asegurada, poder sancionador propio y revisión judicial de sus resoluciones. Este debate se resolverá presumiblemente durante los diálogos a tres, considerando también la conexión con la tramitación del Reglamento Europol, que ofrece un debate de similares características en lo tocante al régimen de supervisión en protección de datos.

D) OTRAS ACTIVIDADES DE LA AEPD EN EL ÁMBITO EUROPEO

La Agencia ha mantenido su participación en el Grupo de Expertos en Retención de Datos en Telecomunicaciones, auspiciado por la Comisión Europea, cuya misión es asesorar a la Comisión y a los Estados miembros en las actividades relacionadas con la implantación efectiva de la Directiva de Retención de Datos en Telecomunicaciones del año 2006. En este grupo participan miembros de las Autoridades competentes para requerir y tratar estos datos, las operadoras de telecomunicaciones y Autoridades nacionales de protección de datos. Este grupo ha comenzado su andadura en el segundo trimestre de 2013, con mandato de trabajo hasta 2018.

Tras la Sentencia del Tribunal de Justicia de la UE declarando nula la Directiva de retención de datos, el trabajo del grupo ha finalizado en la práctica, si bien se han celebrado reuniones dirigidas a evaluar el contenido de la sentencia, su posible impacto en las legislaciones nacionales que la desarrollan y posibles alternativas.

Asimismo, la Agencia sigue participando, junto con Alemania, Francia, Holanda y Reino Unido, en el Grupo de Expertos que, a propuesta de la Comisión Europea y en el marco del proceso dirigido a

<Índice>

un eventual reconocimiento como país con nivel de protección adecuado, asesorará a las Autoridades de India en materia de protección de datos. El comienzo de los trabajos del Grupo de Expertos se retrasó debido a la tardanza por parte de las Autoridades de India en constituir a su propio grupo de expertos (que ya ha comenzado a funcionar en 2014), habiéndose celebrado una primera reunión con la representación india así como varias reuniones del Grupo de Expertos. Aunque estaba prevista una reunión en la India en el mes de septiembre, diversas dificultades surgidas del lado de su representación obligaron a posponerla, sin que por el momento haya fecha prevista para su realización.

En el marco de los proyectos del programa marco de investigación FP7 de la Unión Europea, la Agencia ha participado con un papel asesor en el ámbito de la protección de datos en los proyectos CIRRUS y PACT, relacionados con la certificación en el ámbito de la computación en nube y en el estudio de la percepción pública del uso de nuevas tecnologías en seguridad, respectivamente.

Es necesario hacer una referencia particular a la participación de la Agencia en las tareas del Grupo Internacional de Protección de Datos en las Telecomunicaciones, conocido como Grupo de Berlín. Creado en 1980, ha prestado a lo largo de los años particular atención a las cuestiones de protección de datos en el ámbito de las Telecomunicaciones y los medios de comunicación, y en particular al impacto en este ámbito del despliegue de nuevas tecnologías. Otra particularidad de relevancia es que se trata de un grupo en el que participan regularmente, además de las Autoridades europeas, las de Canadá y Estados Unidos, Japón y Corea, así como Australia, Nueva Zelanda y varias Autoridades de América del Sur. De esta forma, los dictámenes de este grupo, aprobados por consenso, mantienen un equilibrio entre las diferentes aproximaciones a la protección de datos en distintas jurisdicciones, lo que confiere a dichos documentos una gran utilidad.

En el año 2014, el Grupo ha celebrado dos reuniones, una en Skopje (Macedonia) y otra en Berlín (Alemania). De entre los trabajos realizados, destaca la adopción de un Dictamen sobre Big Data y privacidad y otro sobre el uso de dispositivos propiedad del usuario en entornos corporativos. En particular, la Opinión sobre Big Data pone el acento en el uso de nuevas técnicas de análisis de datos que permiten la explotación del flujo masivo de información generada en diversos entornos, ofreciendo un conjunto de recomendaciones referidas a los procedimientos de obtención del consentimiento, el uso de técnicas de anonimización, las prácticas que favorecen la transparencia hacia el usuario y los procedimientos de adopción de técnicas de privacidad desde el diseño.

Finalmente, es de destacar que la Agencia se ha incorporado a los trabajos del Privacy Risk Framework Project Workshop. El Proyecto está promovido por el Center for Information Policy Leadership y sigue las mismas líneas que la anterior iniciativa de este *think tank*, el Accountability Project, con reuniones de expertos procedentes de la industria y del entorno de las Autoridades de protección de datos cuyos resultados se plasman en documentos elaborados por el Center que se van refinando según la evolución de las discusiones. El proyecto pretende analizar el papel que la noción de riesgo puede desempeñar en el diseño y la ejecución de políticas de privacidad en las organizaciones, y se enmarca entre las diversas propuestas que se han mencionado anteriormente al hacer alusión a la Declaración del GT29 sobre el *risk based approach*. Durante 2014 se han celebrado dos reuniones del Proyecto, una en París y otra en Bruselas.

E) CONFERENCIA DE PRIMAVERA DE AUTORIDADES EUROPEAS DE PROTECCIÓN DE DATOS

El 5 de junio se celebró en Estrasburgo la Conferencia de Primavera de Autoridades europeas de protección de datos, organizada conjuntamente por la Autoridad francesa de protección de datos (CNIL) y el delegado de protección de datos del Consejo de Europa.

La Conferencia giró en torno al tema de la cooperación entre las autoridades de protección de datos, tanto en el ámbito europeo como internacional.

La Agencia Española fue ponente en una de las cuatro mesas redondas en que se estructuró la conferencia, dedicada a las expectativas de los diferentes actores implicados en los procesos de supervisión. En el caso de la Agencia, la presentación giró en torno a las expectativas de las autoridades de protección de datos.

Como consecuencia de la Conferencia, se ha lanzado un Grupo de Trabajo de Cooperación en materia de Cumplimiento de la Ley (*enforcement*), que tiene como objetivo el desarrollo de mecanismos que permitan la cooperación entre los miembros de la Conferencia (lo que incluye tanto a Estados de la UE como de fuera de ella) en temas de inspección y sanción por incumplimientos de la normativa de protección de datos. La AEPD forma parte de ese Grupo de Trabajo, que deberá presentar sus conclusiones a la próxima Conferencia, que se celebrará en Manchester. Puede destacarse que entre esas conclusiones está previsto abordar la implantación de un sistema seguro de intercambio de información entre las autoridades participantes cuya infraestructura, según lo avanzado por la Autoridad francesa, podría ser proporcionada por la Comisión Europea, aunque no hay una decisión definitiva al respecto.

F) CONFERENCIA INTERNACIONAL DE COMISIONADOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Entre los días 13 y 16 de octubre de 2014 se celebró en Mauricio la 36ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, bajo el lema «Un orden mundial para la protección de datos: ¿Nuestro sueño hecho realidad?»

En esta edición, y siguiendo los criterios adoptados en la Conferencia de México y ya aplicados en las de Punta del Este y Varsovia, la Sesión Cerrada tuvo un elevado peso específico en el conjunto de la Conferencia, dedicando un día al estudio y debate del Internet de las Cosas. El resultado de estos debates se ha plasmado en la Declaración de Mauricio, que contiene diversas propuestas y recomendaciones para hacer frente al impacto sobre la protección de datos de la cada vez mayor presencia de objetos inteligentes en el entorno cotidiano. Es interesante resaltar que las contribuciones de las Autoridades europeas presentes en la Conferencia reflejaron en todos los casos los contenidos del Dictamen del GT29 en la materia, en el que la AEPD actuó como ponente.

La Conferencia adoptó también una serie de resoluciones, entre las que pueden destacarse una relativa a Big Data y otra sobre Cooperación en materia de *enforcement* del derecho de protección de datos y privacidad. Esta última iba acompañada de, y giraba en torno a, un Global Cross Border Enforcement Cooperation Arrangement, un acuerdo de cooperación transfronteriza en medidas de aplicación de la ley en el ámbito de la protección de datos de carácter personal y la privacidad. Este documento fue preparado por el Grupo de Trabajo creado

<Índice>

en la Conferencia de México, que con él cumplía su mandato. Pretende ofrecer una aproximación multilateral y unos mecanismos de cooperación y coordinación para facilitar el intercambio de información, incluida la confidencial, entre autoridades de privacidad y protección de datos para responder de una manera más efectiva a vulneraciones transnacionales acerca de estas materias. El «Arreglo» («*Arrangement*») no genera ninguna obligación en derecho internacional y la adhesión al mismo es voluntaria. Igualmente, los participantes pueden declinar demandas de cooperación de otros participantes por cualquier motivo razonable, sin mayor requisito que explicar las causas de la negativa. Los principales aspectos del documento tienen que ver con las garantías para el manejo de la información que se intercambia, especialmente cuando tal información tiene carácter confidencial en virtud de la legislación del país que la proporciona.

En esta Conferencia fueron reconocidos como nuevos miembros las Autoridades de protección de datos de Bremen (Alemania), Ghana y Senegal. Fueron también acreditadas como observadores entidades de Bermudas, Japón, Estado de México (México), Singapur y Estados Unidos que desarrollan funciones que se relacionan con la protección de datos.

Aunque el Grupo de Trabajo de Coordinación Internacional para *enforcement* ha quedado disuelto, la antes citada Resolución prevé que anualmente siga ofreciéndose una oportunidad a los miembros de la Conferencia especialmente interesados en el tema de la cooperación para reunirse a debatir específicamente sobre estas cuestiones. En 2014 esa reunión anual se ha celebrado en Manchester (Reino Unido) y Canadá se ofreció para acoger la edición de 2015 en Otawa (Canadá).

El Comité Ejecutivo ha visto modificada su composición. Por una parte, la autoridad holandesa cesó como miembro y en la presidencia del Comité, si bien seguirá integrándolo durante dos años más al corresponderle automáticamente por el hecho de ser la organizadora de la siguiente Conferencia Internacional, que tendrá lugar en Ámsterdam. Polonia también ha abandonado el Comité, al que se incorporó como organizadora de la anterior Conferencia de Varsovia. Finalmente, Francia fue elegida como nuevo miembro, en sustitución de Holanda. El Comité Ejecutivo se compone, por tanto, de las autoridades de Mauricio y Holanda, en su condición de organizadores de la última y la siguiente Conferencia, y de EEUU, Nueva Zelanda y Francia. La autoridad de Nueva Zelanda presentó una única candidatura para suceder a Holanda en la presidencia, siendo unánimemente aceptada como tal en la Sesión Cerrada.

El Director de la AEPD participó como moderador y ponente en un panel de la Sesión Abierta de la Conferencia dedicado al tema «Ventanilla Única: Centralización vs. Proximidad». Asimismo, la representación de la AEPD intervino en las actividades paralelas organizadas por la GPEN (Red Global de Control de la Privacidad, por sus siglas en inglés), los proyectos PHAEDRA y el Grupo de Trabajo de la Conferencia sobre Educación Digital.

G) LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

En lo referente al desarrollo legislativo, durante el año 2014 no se han producido novedades en cuanto a la aprobación de leyes generales de protección de datos personales. Sí, en cambio, las ha habido en ámbitos directamente vinculados con esta materia, como los relativos a la transparencia y el acceso a la información pública. En este sen-

tido, hay que destacar la aprobación en Colombia de la Ley 1712, de 6 de marzo, de Transparencia y del Derecho de Acceso a la Información Pública nacional, y la entrada en vigor en España de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, con la puesta en marcha del Consejo de Transparencia y Buen Gobierno.

En cuanto a la normativa aún en proyecto, deben reseñarse iniciativas legislativas en Brasil, Chile y Honduras, que se encuentran en distintas fases de desarrollo. Así, por lo que se refiere a Brasil, viene tramitándose en sede gubernamental desde hace más de un año un anteproyecto de ley de regulación general en la materia, que tras la pausa sufrida durante las elecciones presidenciales a finales de 2014, vuelve a cobrar impulso, fomentando sus promotores un amplio debate nacional sobre el mismo. De otra parte, durante el mes de septiembre de 2014 se ha presentado por parte del Ministerio de Economía de Chile un anteproyecto de Ley general en la materia, que derogaría la vigente Ley del año 1999. Dicho texto se ha sometido a consulta pública y continúa tramitándose en sede gubernamental. Finalmente, a instancias del Instituto de Acceso a la Información Pública, se está impulsando un anteproyecto de ley general en la materia en Honduras que, una vez se someta a la valoración de expertos y colectivos de los sectores más implicados (salud, banca o crédito, entre otros), se pretende remitir en breve para su tramitación parlamentaria.

Respecto a las actividades de la Red Iberoamericana de Protección de Datos (RIPD), hay que destacar, en primer término, la celebración del XII Encuentro Iberoamericano de Protección de Datos, que tuvo lugar en la ciudad de México del 11 al 14 de noviembre, en la sede del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI). Al mismo asistieron miembros de la RIPD de Argentina, Brasil, Chile, Colombia, Ecuador, El Salvador, España, Guatemala, Honduras, México, Perú, Portugal, República Dominicana y Uruguay, así como representantes de la Organización de Estados Americanos (OEA) y de FIIAPP-EUROsociAL, junto con una destacada presencia del sector privado, especialmente grandes empresas prestadoras de servicios de internet y telecomunicaciones,

<Índice>

profesionales y expertos en los distintos ámbitos tratados en el evento.

El primer día del Encuentro se desarrolló un programa de capacitación que contó con la presencia de empleados y directivos de los Institutos estatales de México y del propio IFAI, que fue impartido por representantes de la AEPD, la Agencia Vasca y Autoridad Catalana de Protección de Datos. Con esta actuación, se pretende iniciar un canal estable de participación de los órganos estatales de México en las actividades de la RIPD mediante la formación y la capacitación bajo la coordinación del IFAI.

El segundo y tercer día se celebró la Sesión Abierta, que contó con una participación de en torno a 700 asistentes. Además, las sesiones se pudieron seguir a través de la página habilitada en la web del IFAI. Durante los dos días de sesiones se registraron un total de 1.593 visitas.

La Sesión Abierta fue inaugurada por la Comisionada-Presidenta del IFAI y por el Director de la AEPD en su condición de titulares de la Presidencia y Secretaría Permanente de la RIPD, respectivamente. El Director de la AEPD intervino, asimismo, como ponente de la Sesión 1, relativa a «La protección de datos personales en internet: la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014». Por su parte, el Adjunto al Director lo hizo como ponente en la Sesión 3, bajo el título «La actividad empresarial y la privacidad. Las transferencias internacionales de datos personales y la convergencia entre sistemas de protección». Otras cuestiones fueron las relativas a la protección de datos personales en el ámbito de las relaciones laborales, las nuevas tecnologías, el modelo mexicano de protección de datos o las principales novedades regulatorias, impartidas por las Autoridades de protección de datos, expertos, docentes, abogados, representantes empresariales y parlamentarios.

En la Sesión Cerrada del Encuentro se debatieron cuestiones internas de la RIPD, como la aprobación del Plan de Trabajo para 2015 y una Declaración sobre el impulso de la Ley Modelo de Protección de Datos de la OEA, con la creación de un Grupo de Trabajo de la RIPD para colaborar en su elaboración. Asimismo, se procedió a la renovación, para los próximos dos años, de la Presidencia de la Red, que ha recaído nuevamente en el IFAI, y del Comité Ejecutivo, que ha quedado integrado por las autoridades de Colombia, Perú y Uruguay, junto con la AEPD, que es miembro nato de este órgano en su condición de Secretaría Permanente de la RIPD. Se acordó finalmente que el XIII Encuentro, en 2015, se celebre en Lima, organizado por la Autoridad Nacional de Protección de Datos de Perú.

El Encuentro concluyó con la aprobación de una Declaración Final en la que se reiteraron y actualizaron los compromisos asumidos por la RIPD[3].

De otra parte, hay que mencionar las actividades organizadas por la RIPD dentro del Programa PIFTE, gestionado por la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), que ha venido apoyando de forma activa a la RIPD desde sus orígenes. En este marco, se desarrolló durante los días 11 a 14 de febrero el taller «El impulso al desarrollo normativo de la protección de datos personales en Centroamérica y El Caribe», en el Centro de Formación de la Cooperación Española, en La Antigua (Guatemala). Con esta actividad se ha pretendido impulsar

[3] Una información más completa y detallada del XII Encuentro (programa, ponencias y declaraciones finales), se encuentra disponible la web www.redipd.org en el apartado de Actividades/Encuentros/XII Encuentro.

el desarrollo de un sistema normativo propio en materia de protección de datos personales en la zona de Centroamérica y El Caribe, que hasta la fecha sólo cuenta con normativa general en Costa Rica y Nicaragua.

En dicho taller se desarrolló un extenso programa de capacitación sobre las diferentes cuestiones que afectan a la regulación de la protección de datos. Fue impartido por el Secretario de Protección de Datos del IFAI, la Secretaría General de la AEPD y una Asesora Jurídica de la Unidad Reguladora y de Control de Datos Personales de Uruguay. Participaron un total de 25 Autoridades y altos funcionarios de instituciones públicas competentes en materia de protección de datos y de acceso a la información pública, del Poder Judicial, de los registros civiles y de otras instancias gubernamentales de Costa Rica, El Salvador, Honduras, Guatemala, Nicaragua, Panamá, Cuba y República Dominicana.

En paralelo a las actividades propiamente formativas, se desarrollaron reuniones entre las Autoridades de protección de datos presentes en el taller y representantes de la OEA para avanzar en los trabajos de elaboración del proyecto de la llamada Ley Modelo de Protección de Datos Personales, una iniciativa regional que pretende aprobar la OEA, con la participación activa de la RIPD. Por parte de la OEA, asistieron el Director y la Abogada principal del Departamento de Derecho Internacional, y el relator del proyecto de Ley Modelo y miembro del Comité Jurídico Interamericano.

Asimismo, dentro del Programa PIFTE, los días 21 a 23 de octubre, tuvo lugar en el Centro de Formación de la Cooperación Española en Santa Cruz de la Sierra (Bolivia) el seminario «La privacidad en el ámbito de las tecnologías de la salud. La Historia Clínica Electrónica». Este evento reunió a un total de 33 representantes de Autoridades de protección de datos y especialistas de la salud de Argentina, Bolivia, Colombia, Costa Rica, Chile, El Salvador, España, Guatemala, Honduras, México, Paraguay y Perú. Durante su celebración los participantes intercambiaron experiencias y conocimientos sobre el impacto de las nuevas tecnologías de la salud en la protección de los datos personales en campos como la historia clínica electrónica, investigación biomédica, biobancos, ensayos clínicos o seguridad de la información clínica. Se expusieron asimismo algunas iniciativas muy novedosas en campos como el Big Data o el Open Data en el tratamiento de los datos de salud. Por último, la OEA expuso el alcance del Programa de Universalización de la Identidad Civil en las Américas (PUICA).

Como novedad, hay que mencionar la ampliación del campo de actuación de la RIPD a través del Programa EUROsociAL, programa regional de cooperación técnica de la Unión Europea con América Latina, para apoyar políticas públicas nacionales dirigidas a mejorar los niveles de cohesión social y fortalecer las instituciones que las lleven a cabo. En España, la gestión de EUROsociAl está liderada por la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), que desde el Encuentro de México ha pasado a ser miembro observador de la RIPD.

En el marco del Programa EUROsociAL, la RIPD participó en el desarrollo del «Taller Internacional sobre Protección de Datos Personales en El Salvador», celebrado los días 6 y 7 de octubre, en San Salvador, a iniciativa del Instituto de Acceso a la Información Pública de El Salvador. Asistieron como ponentes miembros de la RIPD de Costa Rica, El Salvador, España, Honduras, México y Perú. Por parte de la AEPD, participó una letrada del Gabinete Jurídico. El objetivo del Taller era impulsar la protección de datos personales en este país, abriendo un espacio

<Índice>

de discusión e intercambio de experiencias y buenas prácticas con vistas a la redacción final de un manual con directrices y lineamientos dirigido a los distintos departamentos e instancias administrativas salvadoreñas. En este mismo marco, desde el 10 al 12 de diciembre tuvo lugar en Tegucigalpa el «Taller Internacional sobre Protección de Datos Personales en Honduras» a instancias del Instituto de Acceso a la Información Pública de Honduras. Asistieron como ponentes representantes de la RIPD de Ecuador, Chile, México y Uruguay. Su objetivo era asesorar al Instituto hondureño en la redacción de su anteproyecto de Ley de protección de datos, promoviendo un debate técnico-jurídico y el apoyo de países con leyes de protección de datos ya aprobadas que puedan aportar sus experiencias en este campo.

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 para garantizar un uso adecuado de la información personal.

Entre estos foros, cabe mencionar la Conferencia Internacional «A un año del Reglamento de la Ley de Protección de Datos Personales», que el día 8 de mayo se celebró en Lima, bajo la iniciativa de la Autoridad Peruana de Protección de Datos Personales de Perú (APDP). En la misma intervinieron el Viceministro, el Director General de la APDP, así como el Adjunto al Director de la AEPD y el Secretario de Protección de Datos del IFAI. Durante los días 5 y 6 de junio tuvo lugar en Pereira (Colombia) el Segundo Congreso Internacional de Protección de Datos, organizado por la Superintendencia de Industria y Comercio de Colombia, en el que intervino el Director de la AEPD con la Conferencia «Protección de Datos y confianza en internet».

Y en el mes de diciembre se desarrolló el Santiago de Chile el Seminario Internacional «Hacia una nueva normativa sobre Protección de Datos Personales en Chile», organizado por la Subsecretaría de Economía y el Consejo para la Transparencia de Chile. El Adjunto al Director participó en uno de los paneles con la ponencia «Nuevas tendencias regulatorias», así como en las Mesas de Trabajo y en diversas reuniones con organizaciones empresariales y profesionales de diversos sectores. El objeto principal del evento era el debate sobre el anteproyecto de ley de protección de datos personales que se está tramitando actualmente en Chile.

En cuanto a las visitas institucionales a la AEPD, del 17 al 20 de marzo se impartió por parte de funcionarios de las áreas de Inspección, Registro General de Protección de Datos y Atención al Ciudadano un completo programa de capacitación a cuatro empleadas del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM) en materia de protección de datos personales en el sector público. De otra parte, el día 18 de septiembre se produjo la visita a la Agencia de una delegación de autoridades y parlamentarios de Chile y de México en el marco del Programa EUROsociAL. La delegación de Chile contó con la presencia del Presidente y el Asesor Jurídico del Consejo para la Transparencia, y cuatro miembros de la Cámara de Diputados. La representación de México estaba integrada por dos Comisionados del IFAI y cuatro miembros del Senado mexicano, entre ellos la Presidenta del Comité de Garantía de Acceso y Transparencia de la Información. Por la AEPD, asistieron el Director, el Adjunto al Director, el Jefe del Área Internacional y el responsable de la Secretaría Permanente de la RIPD.

5 COLABORACIÓN INSTITUCIONAL CON EL DEFENSOR DEL PUEBLO

Durante 2014 se han tramitado un total de 53 asuntos promovidos ante esta Agencia por el Defensor del Pueblo. También se han atendido cuatro asuntos planteados por los Defensores del Pueblo de Navarra, Canarias y Galicia.

En cuanto a las principales materias o temas objeto de las peticiones del Defensor del Pueblo, el bloque más destacado es el relativo a videovigilancia, con 12 asuntos, seguido de las cuestiones referentes a los llamados ficheros de morosidad y las empresas de gestión de cobro de deudas, con siete casos; la publicidad telefónica y, en general, las comunicaciones comerciales no deseadas —el llamado spam—, con cinco; y la cesión indebida de datos, con cuatro.

El resto de asuntos hacen referencia a cuestiones de muy variada índole, como el acceso al Registro General de Protección de Datos, el acceso indebido a ficheros de clientes de operadores de telefonía, el acceso a la historia clínica, los llamados contadores inteligentes o las facturaciones erróneas en consumos energéticos.

Los asuntos planteados por los Defensores del Pueblo de Navarra y Canarias se referían a la protección de datos de menores en el ámbito escolar (grabación de imágenes sin consentimiento y difusión de encuesta en centros educativos), y el de Galicia a la difusión de información personal en una web de una organización política. En todos los casos se llevaron a cabo las correspondientes investigaciones y comprobaciones, incluyendo en algún caso visita de inspección (Navarra).

De otra parte, atendiendo a los motivos que llevan a los ciudadanos a obtener información a través del Defensor del Pueblo, el bloque más numeroso es el referido al estado de tramitación de las reclamaciones planteadas ante la Agencia, en 34 ocasiones. 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, en siete casos, o para poder establecer criterios sobre la cuestión suscitada, en cuatro. Así ha ocurrido, por ejemplo, en relación con la publicidad telefónica, los ficheros de morosidad, los contadores inteligentes, o el llamado derecho al olvido.

En otros casos, la queja ante el Defensor del Pueblo se utiliza para manifestar la disconformidad de los afectados con los criterios establecidos por la Agencia, o se trata de una verdadera denuncia o reclamación por presunta infracción de la normativa de protección de datos que debería haberse instado, en su caso, ante la AEPD, y así se ha puesto en conocimiento del afectado.

6 COOPERACIÓN CON LAS AGENCIAS AUTONÓMICAS

Con el fin de garantizar la igualdad de los ciudadanos en relación con el derecho fundamental a la protección de datos personales, los directores de la AEPD, la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos han mantenido dos reuniones para intercambiar información y coordinar criterios sobre la aplicación de la normativa. Asimismo, dichas autoridades han participado conjuntamente en diversos eventos internacionales en Latinoamérica, difundiendo sus experiencias en esta materia.

Además, se ha impulsado la cooperación entre los Registros de las tres entidades con objeto de eliminar trabas y facilitar el cumplimiento de las obligaciones de notificación de los ficheros. Conforme al protocolo de intercambio de operaciones registrales se tramitaron un total de 6.243 operaciones, en su mayor parte correspondientes a altas de ficheros, que han supuesto un incremento de un 219% con respecto a 2013. Entre ellas destacan las altas de ficheros inscritos por las correspondientes administraciones locales, con un incremento de más de un 21% en las del País Vasco, así como las de los ficheros de los que es responsable la Administración de la Comunidad Autónoma del País Vasco.

<Índice>

MEMORIA AEPD 2014

LA AGENCIA EN CIFRAS

<Índice>

1 INSPECCIÓN DE DATOS

DENUNCIAS Y RECLAMACIONES REGISTRADAS

TIPO	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Escritos de reclamación de tutela	2.193	1.997	**2.099**	17,24	5,11
Escritos de denuncia	8.594	8.607	**10.074**	82,76	17,04
TOTAL	10.787	10.604	**12.173**	100	14,80

DENUNCIAS Y RECLAMACIONES RESUELTAS

TIPO	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Reclamaciones de tutela de derechos	2.163	2.108	**1.818**	16,20	–13,76
Denuncias	8.832	8.633	**9.404**	83,80	8,93
TOTAL	10.995	10.741	**11.222**	100	4,48

<Índice>

RESOLUCIONES – EJERCICIO DE LA POTESTAD SANCIONADORA

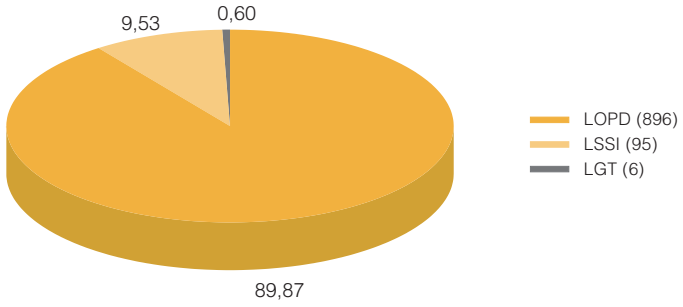
SEGÚN TIPO DE PROCEDIMIENTO	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Desistimiento por art. 42 y 71 LRJPAC	448	415	**467**	5,53	12,53
Acuerdo de inadmisión a trámite	4.756	5.114	**5.692**	67,42	11,30
Archivo de actuaciones de inspección	1.153	1.087	**1.157**	13,70	6,44
Resolución de procedimientos de apercibimiento	316	219	**315**	3,73	43,84
Resolución de procedimientos sancionadores	646	719	**752**	8,91	4,59
Resolución de procedimientos de infracción de las AAPP	38	58	**60**	0,71	3,45

SEGÚN SENTIDO DE LA RESOLUCIÓN	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Archivo actuaciones previas	6.357	6.616	**7.316**	86,65	10,58
Archivo de procedimiento de apercibimiento	10	13	**127**	1,50	876,92
Archivo de procedimiento sancionador	89	103	**113**	1,34	9,71
Archivo de procedimiento de infracción de las AAPP	5	6	**15**	0,18	150
TOTAL RESOLUCIONES DE ARCHIVO	6.461	6.738	**7.571**	89,67	12,36
Declarativa de infracción con apercibimiento	306	206	**207**	2,45	0,49
Declarativa de infracción con sanción económica	557	616	**620**	7,34	0,65
Declarativa de infracción de las AAPP	33	52	**45**	0,53	–13,46
TOTAL RESOLUCIONES DECLARATIVAS DE INFRACCIÓN	896	874	**872**	10,33	–0,23
TOTAL RESOLUCIONES POTESTAD SANCIONADORA	**7.357**	**7.612**	**8.443**	**100**	**10,92**

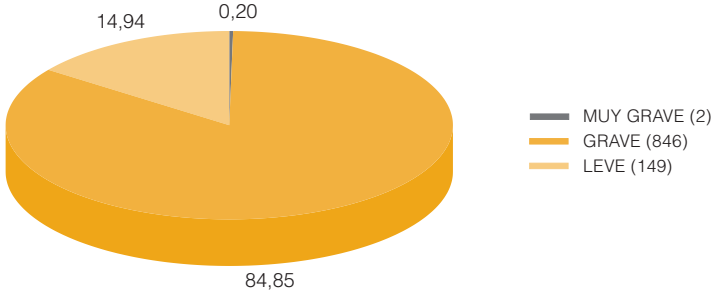
* En cada resolución puede haberse analizado más de una infracción.

1

INFRACCIONES SEGÚN LEY INFRINGIDA



NÚMERO DE 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.

APLICACIÓN DE CRITERIOS DE GRADUACIÓN EN LA DECLARACIÓN DE INFRACCIONES

	2012	2013	2014				% RELATIVO	Δ % 2013/2014
			LOPD	LSSI	LGT	TOTAL		
Apercibimiento	352	216	**194**	**27**	**0**	**221**	22,17	2,31
Sanción escala gravedad precedente	308	350	**442**	**0**	**0**	**442**	44,33	26,29
Sanción sin atenuación	405	418	**260**	**68**	**6**	**334**	33,50	–20,10
TOTAL INFRACCIONES	1.065	984	**896**	**95**	**6**	**997**	100	1,32

* 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

	2012	2013	2014	Δ% 2013/2014
Total sanciones	713	768	**776**	1,04

* 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.

1

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS INICIADAS

ACTIVIDAD	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Telecomunicaciones	2.652	2.256	**2.220**	27,52	–1,60
Entidades financieras	1.077	1.566	**1.540**	19,09	–1,66
Videovigilancia	1.271	918	**966**	11,97	5,23
Servicios de Internet (excepto *spam)*	404	424	**447**	5,54	5,42
Comunicaciones electrónicas comerciales – *spam* (LSSI)	353	344	**353**	4,38	2,62
Publicidad y prospección comercial (excepto *spam)*	241	270	**314**	3,89	16,30
Administración pública	267	360	**311**	3,85	–13,61
Suministro y comercialización de energía/agua	393	346	**237**	2,94	–31,50
Profesionales, admón. fincas, comunidades de propietarios	221	204	**232**	2,88	13,73
Sanidad	151	139	**225**	2,79	61,87
Seguridad privada	9	8	**161**	2,00	1.912,50
Recursos humanos, asuntos laborales	161	160	**147**	1,82	–8,13
Comercio, transporte, hostelería	121	162	**145**	1,80	–10,49
Asociaciones, federaciones, colegios profesionales, clubes, fundaciones, ONG	101	100	**105**	1,30	5
Inscripción de ficheros / Información artículo 5	101	94	**101**	1,25	7,45
Seguros	59	67	**81**	1,00	20,90
Medios de comunicación	62	98	**75**	0,93	–23,47
Cookies (LSSI)	–	16	**58**	0,72	262,50
Asuntos relacionados con procedimientos judiciales	46	62	**56**	0,69	–9,68
Partidos políticos	24	40	**56**	0,69	40
Enseñanza	45	50	**53**	0,66	6
Fuerzas y cuerpos de seguridad	29	47	**49**	0,61	4,26
Sindicatos	48	48	**44**	0,55	–8,33
Documentación desechada sin destruir o borrar	32	29	**39**	0,48	34,48
Comunicaciones comerciales por fax (LGT)	8	9	**16**	0,20	77,78
Derechos ARCO	11	4	**1**	0,01	–75
Otros	77	36	**36**	0,45	0
TOTAL ACTUACIONES PREVIAS INICIADAS	7.964	7.857	**8.068**	100	2,69

* 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 que, tras ser analizadas, no se admiten a trámite (IT).

** En 2014 se incrementó considerablemente el número de denuncias contra compañías de seguridad privada, relacionadas con la inclusión de datos de clientes en ficheros comunes de morosidad.

<Índice>

DISTRIBUCIÓN DE LOS PROCEDIMIENTOS SANCIONADORES RESUELTOS

ACTIVIDAD	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Telecomunicaciones	321	377	**310**	41,22	–17,77
Entidades financieras	90	74	**124**	16,49	67,57
Comunicaciones electrónicas comerciales – *spam* (LSSI)	49	67	**75**	9,97	11,94
Suministro y comercialización de energía/agua	32	54	**63**	8,38	16,67
Videovigilancia	63	57	**39**	5,19	–31,58
Servicios de Internet (excepto *spam)*	24	29	**36**	4,79	24,14
Publicidad y prospección comercial (excepto *spam)*	12	24	**32**	4,26	33,33
Cookies (LSSI)	–	–	**19**	2,53	–
Comercio, transporte, hostelería	8	6	**15**	1,99	150
Seguros	7	7	**8**	1,06	14,29
Recursos humanos, asuntos laborales, sindicatos	3	2	**7**	0,93	250
Inscripción de ficheros / Información artículo 5	1	1	**5**	0,66	400
Asociaciones, federaciones, colegios profesionales, clubes, ONG, fundaciones	3	5	**4**	0,53	–20
Sanidad	2	1	**3**	0,4	200
Comunicaciones comerciales por fax (LGT)	3	4	**1**	0,13	–75
Partidos políticos	5	3	**1**	0,13	–66,67
Profesionales, comunidades de propietarios, Admón. fincas	1	2	**1**	0,13	–50
Otros	22	6	**9**	1,2	50
TOTAL RESOLUCIONES (PS)	646	719	**752**	100	4,59

* 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	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Videovigilancia	235	131	**176**	55,87	34,35
Servicios de Internet (excepto *spam)*	17	19	**34**	10,79	78,95
Profesionales, comunidades de propietarios, admón. fincas	14	11	**18**	5,71	63,64
Comunicaciones electrónicas comerciales – *spam* (LSSI)	–	–	**14**	4,44	–
Documentación desechada sin destruir o borrar	5	4	**12**	3,81	200
Asociaciones, federaciones, colegios profesionales, clubes	12	14	**9**	2,86	–35,71
Comercio, transporte, hostelería	5	13	**8**	2,54	–38,46
Cookies (LSSI)	–	–	**5**	1,59	–
Enseñanza	6	–	**5**	1,59	–
Publicidad y prospección comercial (excepto *spam)*	1	5	**5**	1,59	0
Recursos humanos, asuntos laborales, sindicatos	2	10	**4**	1,27	–60
Telecomunicaciones	–	–	**4**	1,27	–
Sanidad	3	4	**4**	1,27	0
Partidos políticos	1	2	**2**	0,63	0
Inscripción de ficheros / Información artículo 5	6	–	**2**	0,63	–
Suministro y comercialización de energía/agua	–	–	**2**	0,63	–
Otros	9	6	**11**	3,49	83,33
TOTAL RESOLUCIONES (A)	316	219	**315**	100	43,84

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

<Índice>

RESOLUCIONES DECLARATIVAS DE INFRACCIÓN (SECTOR PRIVADO)

ACTIVIDAD	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Telecomunicaciones	289	317	**270**	32,65	–14,83
Videovigilancia	276	176	**158**	19,11	–10,23
Entidades financieras	77	62	**98**	11,85	58,06
Comunicaciones electrónicas comerciales – *spam* (LSSI)	39	59	**74**	8,95	25,42
Suministro y comercialización de energía/agua	29	48	**52**	6,29	8,33
Servicios de internet (excepto *spam*)	39	44	**50**	6,05	13,64
Publicidad y prospección comercial (excepto *spam*)	10	29	**30**	3,63	3,45
Cookies	–	–	**20**	2,42	–
Comercio, transporte, hostelería	9	15	**17**	2,06	13,33
Recursos humanos, asuntos laborales, sindicatos	14	10	**9**	1,09	–10
Profesionales, comunidades de propietarios, Admón. fincas	15	11	**8**	0,97	–27,27
Seguros	9	6	**8**	0,97	33,33
Asociaciones, federaciones, colegios profesionales, clubes, ONG, fundaciones	15	19	**7**	0,85	–63,16
Inscripción de ficheros / Información artículo 5	7	1	**5**	0,6	400
Sanidad	5	5	**3**	0,36	–40
Partidos políticos	4	5	**3**	0,36	–40
Documentación desechada sin destruir o borrar	2	4	**3**	0,36	–25
Enseñanza	6	0	**2**	0,24	–
Administración pública (entidades Derecho privado)	2	0	**2**	0,24	–
Medios de comunicación	2	1	**1**	0,12	0
Otros	9	6	**7**	0,85	0
TOTAL RESOLUCIONES DECL. INFRACCIÓN (PS, A)	863	822	**827**	100	0,61

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

1

SANCIONES ECONÓMICAS IMPUESTAS

ACTIVIDAD	2012	2013	2014	Δ% 2013/2014
TOTAL SANCIONES	21.054.656,02	22.339.440	**17.002.622**	–23,89

SECTORES CON MAYOR IMPORTE GLOBAL DE SANCIONES

PROCEDIMIENTOS DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS RESUELTOS

TIPO ADMINISTRACIÓN	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Local	22	28	**32**	53,33	14,29
General del Estado	4	9	**14**	23,33	55,56
Autonómica	12	20	**12**	20	–40
Otras Entidades de Derecho Público	0	1	**2**	3,33	100
TOTAL RESOLUCIONES	38	58	**60**	100	3,45

* En un mismo procedimiento de infracción pueden figurar imputados de distintas administraciones territoriales, computándose tales procedimientos en una sola de las administraciones afectadas.
** Se incluyen tanto las resoluciones que declaran infracción como las de archivo del procedimiento.

<Índice>

INFRACCIONES DECLARADAS DE LAS ADMINISTRACIONES PÚBLICAS

TIPO DE ADMINISTRACIÓN	2012	2013	2014	% RELATIVO	Δ% 2013/2014
Local	22	26	**27**	52,94	3,85
Autonómica	13	21	**12**	23,53	–42,86
General del Estado	5	9	**11**	21,57	22,22
Otras Entidades de Derecho Público	0	1	**1**	1,96	0
TOTAL INFRACCIONES	40	57	**51**	100	–10,53

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

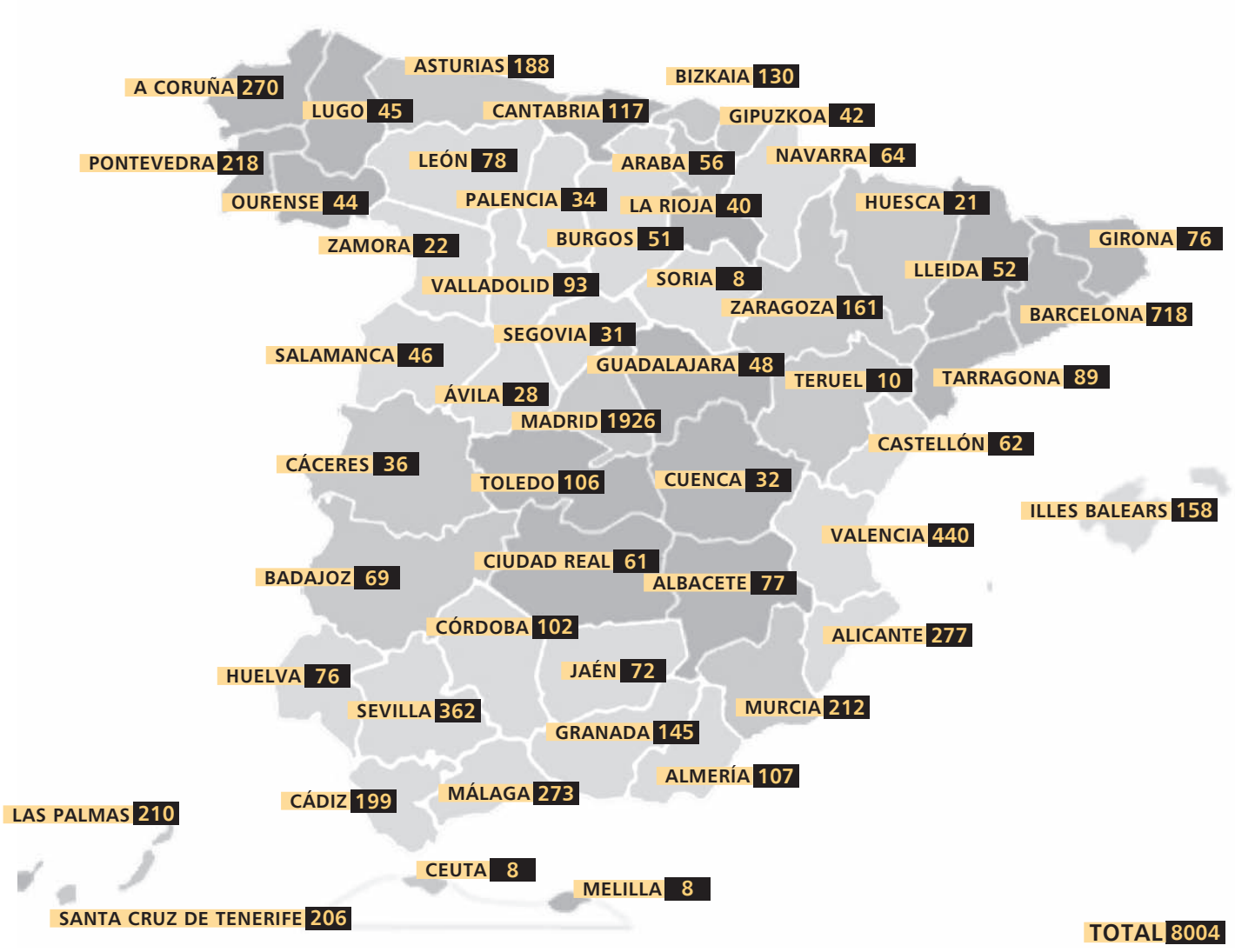
PROCEDIMIENTOS DE TUTELA DE DERECHOS RESUELTOS

	ESTIMATORIA	ESTIMATORIA FORMAL O PARCIAL	DESESTIMATORIA	ARCHIVO POR INADMISIÓN O DESISTIMIENTO	TOTAL
Cancelación	186	140	145	576	1.047
Acceso	165	130	91	213	599
Rectificación	11	18	12	45	86
Oposición	29	21	13	73	136
TOTAL	**391**	**309**	**261**	**907**	**1.868**

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

1

DISTRIBUCIÓN GEOGRÁFICA DE LAS ACTUACIONES PREVIAS INICIADAS EN 2014 (PROVINCIA DEL DENUNCIANTE)

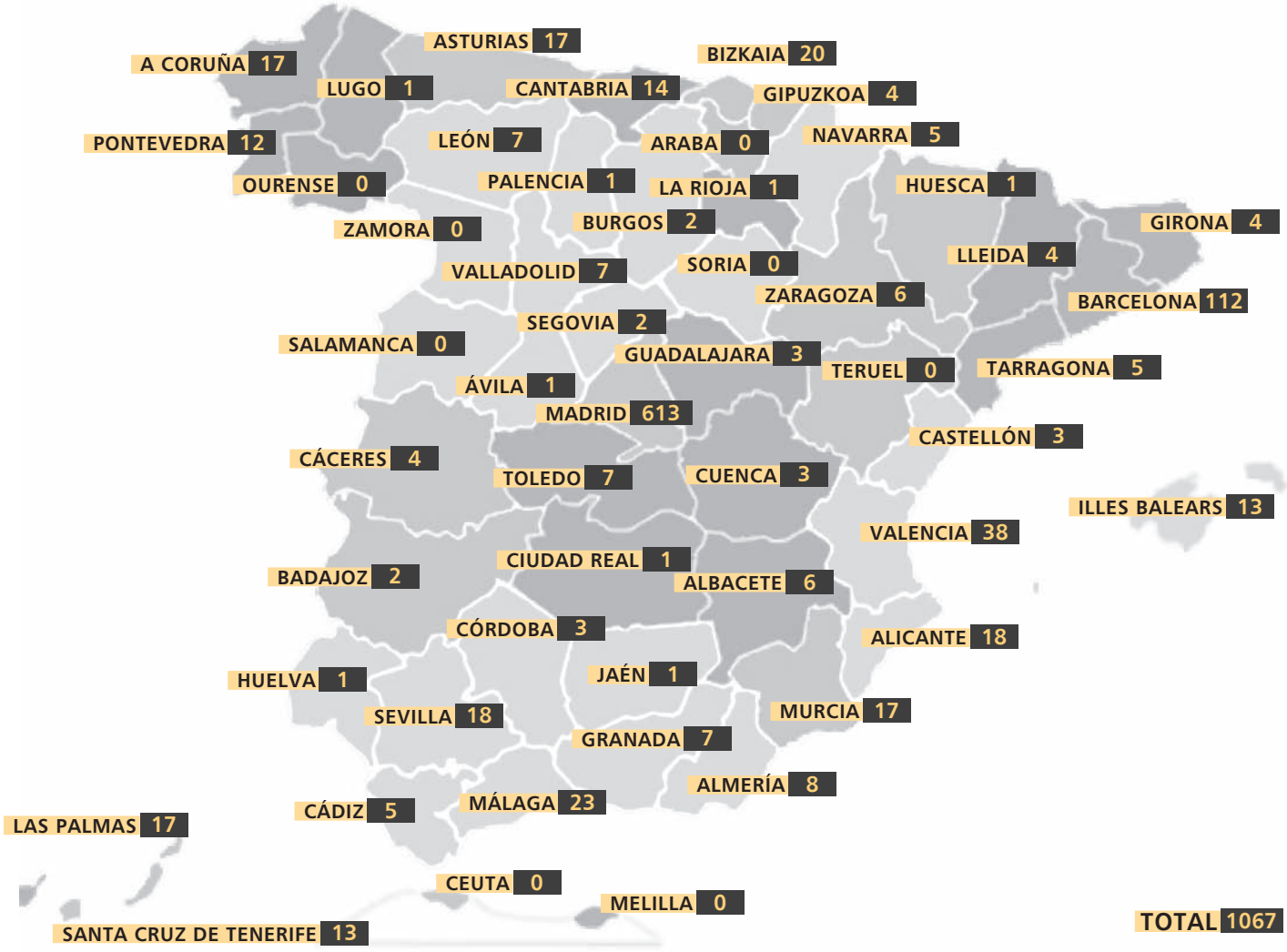


* No se consideran las actuaciones previas iniciadas de oficio a iniciativa del Director o las iniciadas por solicitud de colaboración de otras autoridades extranjeras de protección de datos.

<Índice>

1

ESTABLECIMIENTO DE IMPUTADOS EN PROCEDIMIENTOS SANCIONADORES Y DE APERCIBIMIENTO RESUELTOS EN 2014



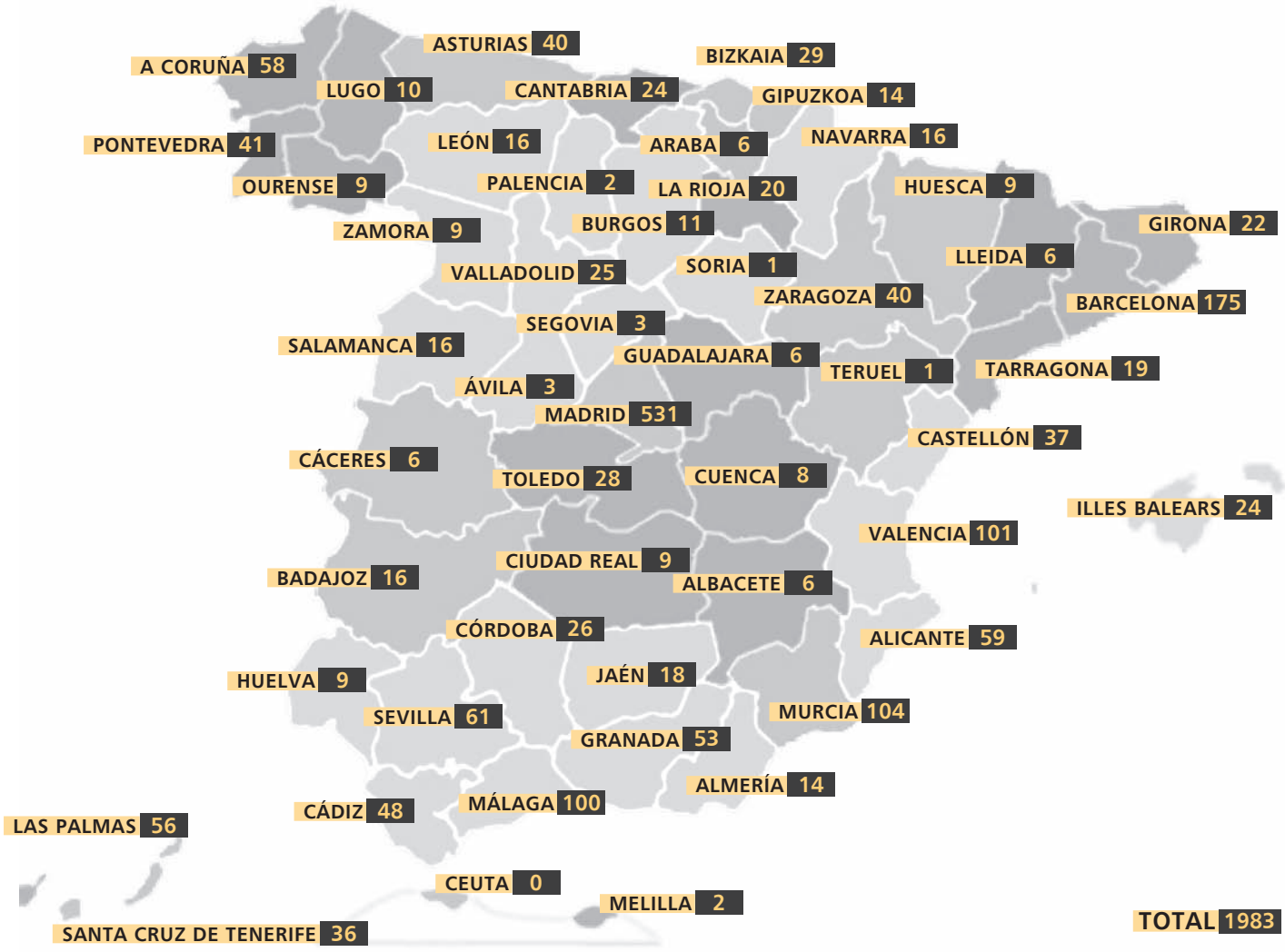
1

SEDE DE LOS IMPUTADOS EN PROCEDIMIENTOS DE DECLARACIÓN DE INFRACCIÓN DE LAS AAPP RESUELTOS EN 2014

TOTAL 60

<Índice>

DISTRIBUCIÓN GEOGRÁFICA DE LOS PROCEDIMIENTOS DE TUTELAS DE DERECHOS INICIADOS EN 2014 (PROVINCIA DEL RECLAMANTE)



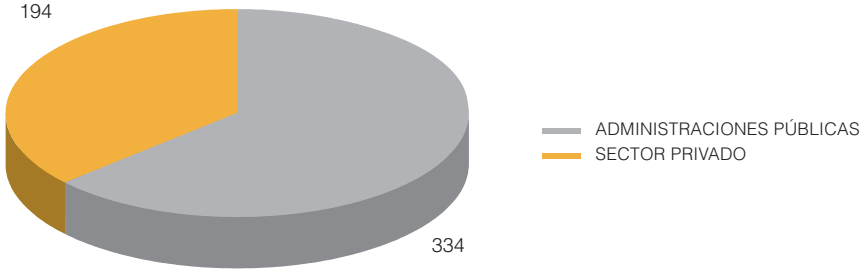
2 GABINETE JURÍDICO

CONSULTAS

ADMINISTRACIONES PÚBLICAS	334
Administración General del Estado	150
Comunidades Autónomas	79
Entidades Locales	51
Otros Organismos Públicos	54

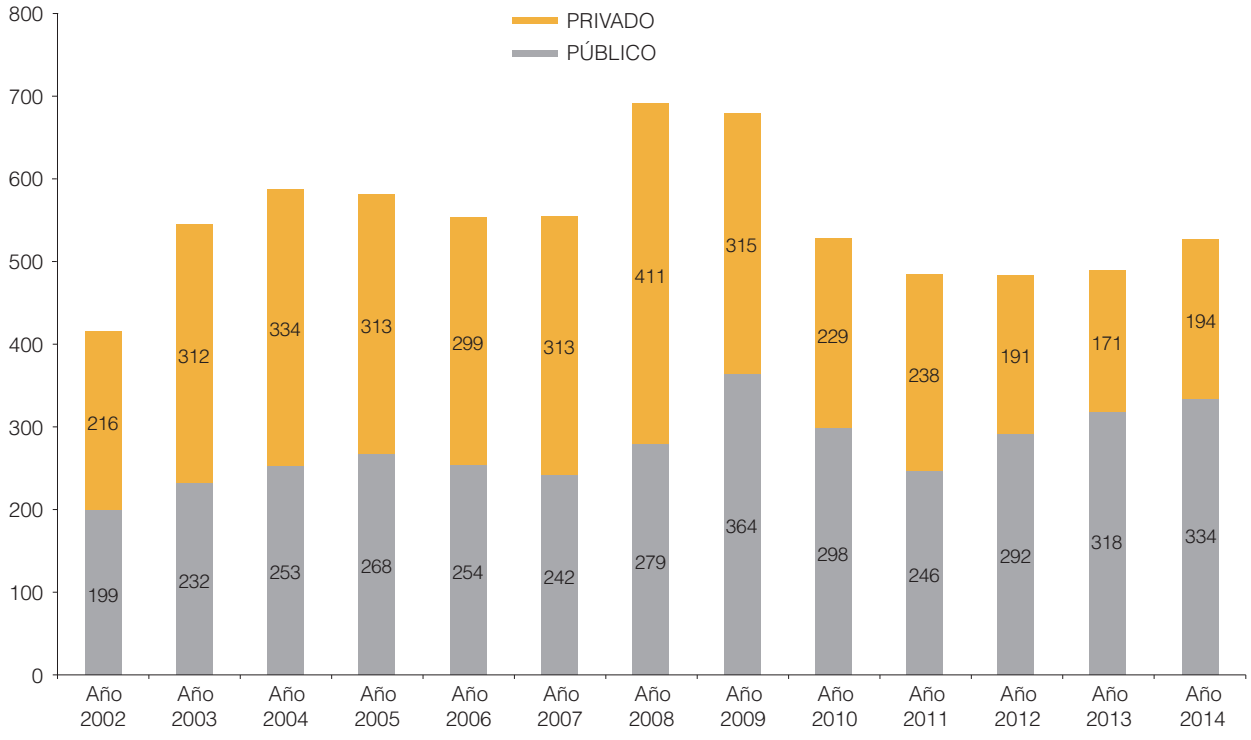
CONSULTAS PRIVADAS	194
Empresas	128
Particulares	31
Asociaciones/Fundaciones	22
Sindicatos/Partidos políticos	12
Otros (Iglesia)	1

DISTRIBUCIÓN 2014 DE CONSULTAS PÚBLICAS/PRIVADAS



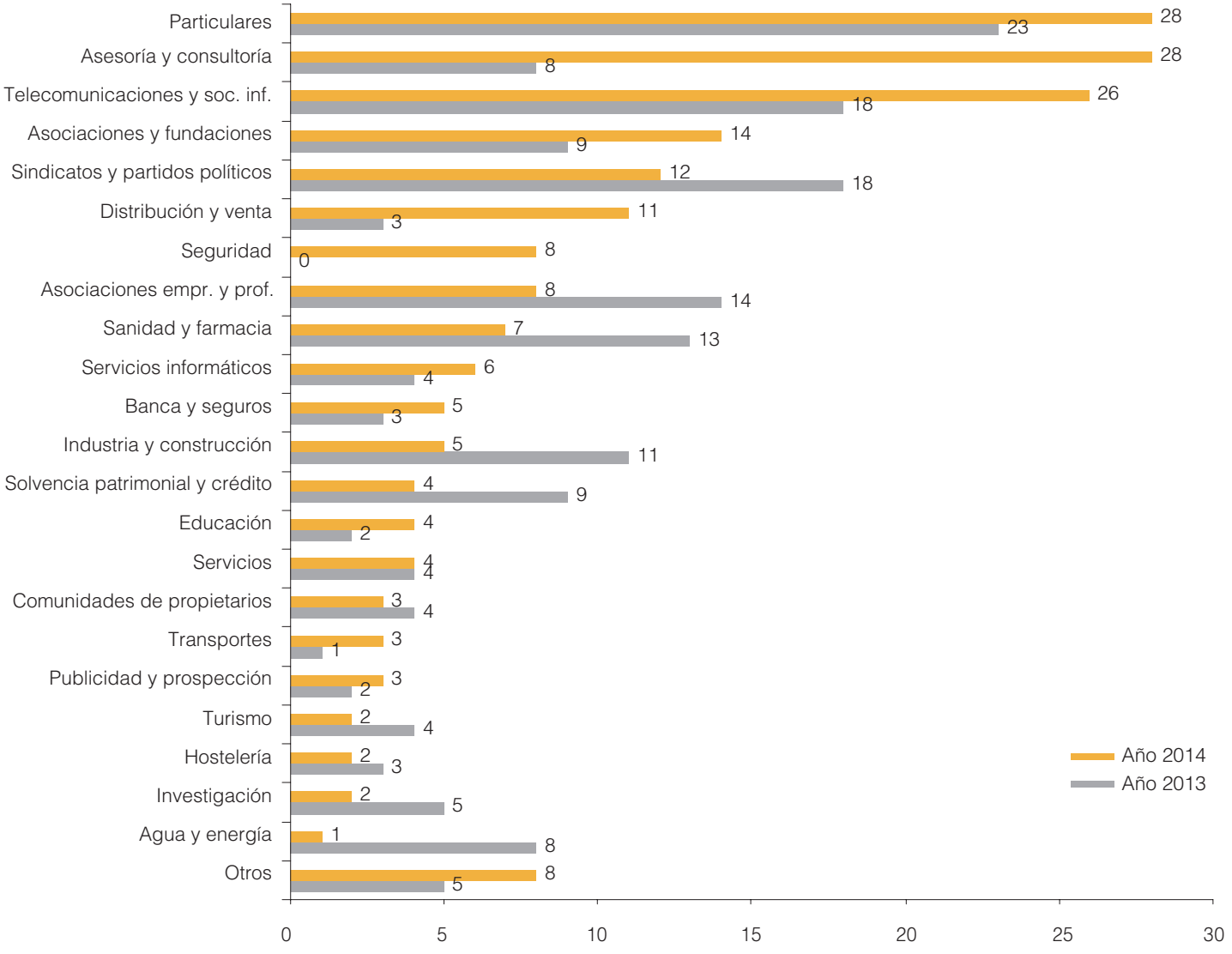
<Índice>

EVOLUCIÓN DE LAS CONSULTAS (2002-2014)



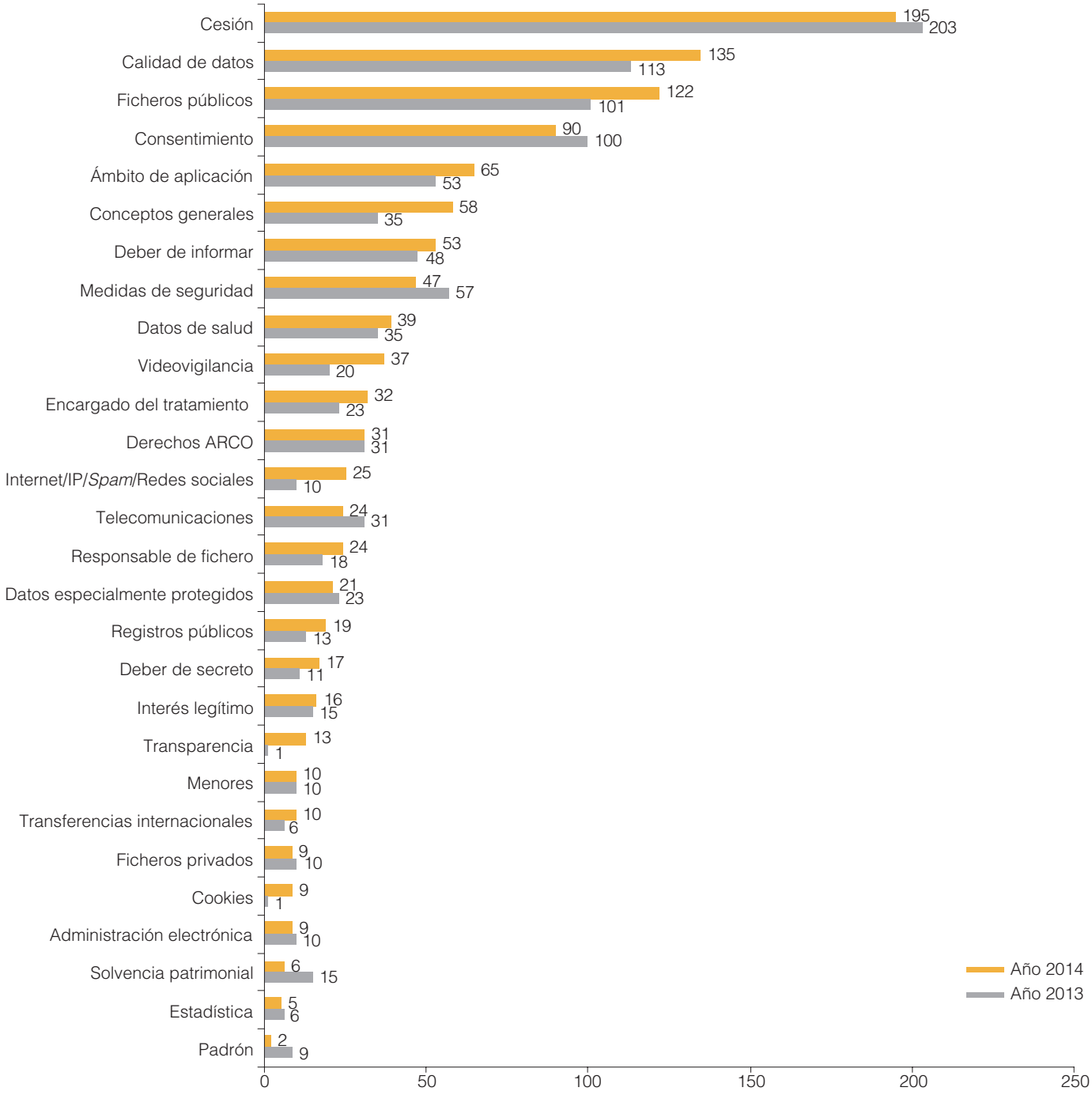
2

EVOLUCIÓN DE LAS CONSULTAS POR SECTORES (2013-2014)



<Índice>

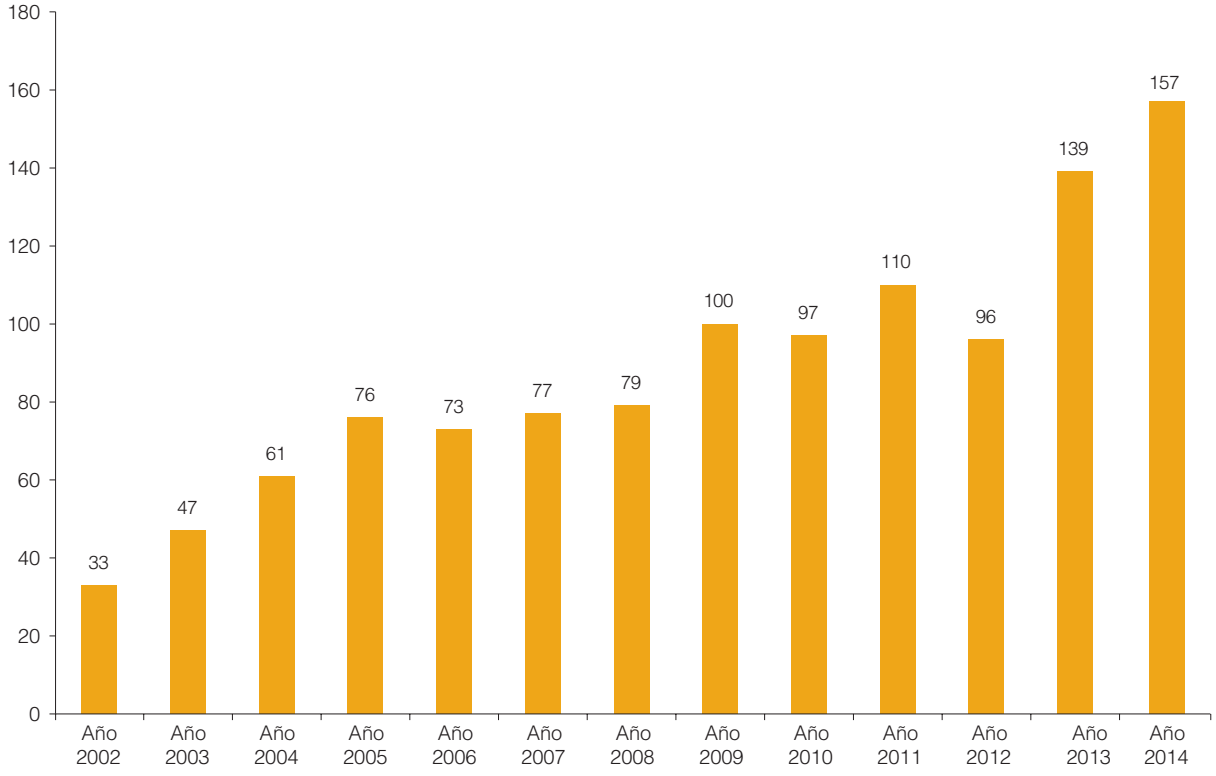
EVOLUCIÓN DE LAS CONSULTAS POR MATERIAS (2013-2014)



<Índice>

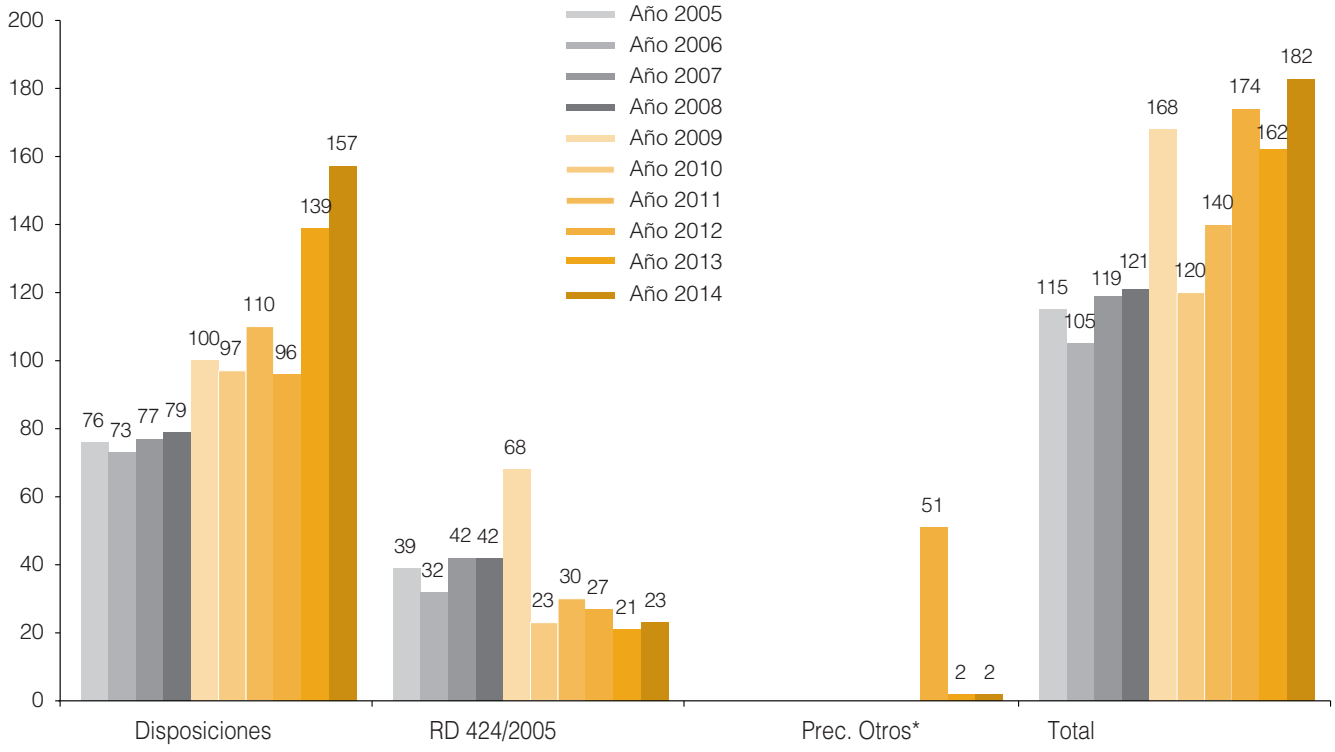
2

EVOLUCIÓN DE INFORMES PRECEPTIVOS A DISPOSICIONES GENERALES (2002-2014)



<Índice>

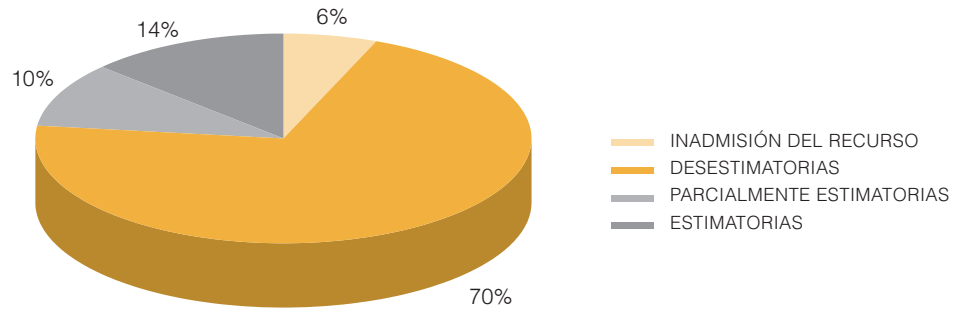
EVOLUCIÓN DE INFORMES PRECEPTIVOS (2005-2014)



* En 2012 y 2013 Ley de Regulación del juego; en 2014 Ley de Prevención del blanqueo de capitales.

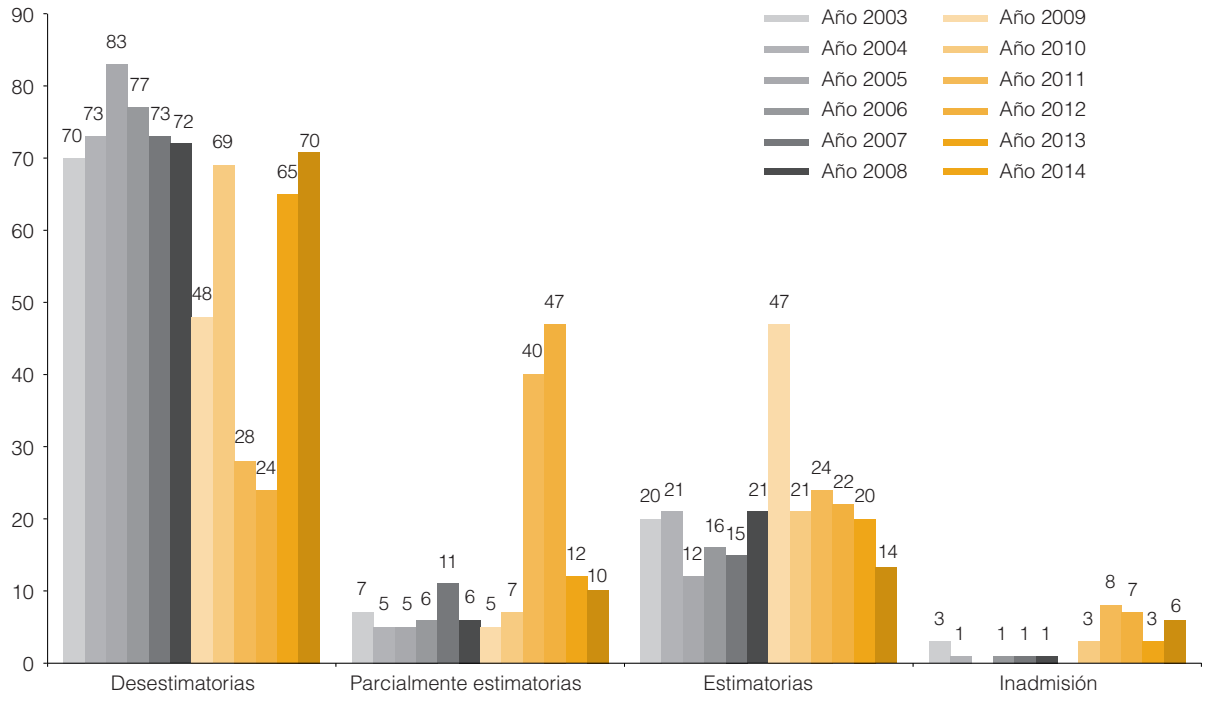
2

SENTENCIAS DE LA AUDIENCIA NACIONAL EN 2014



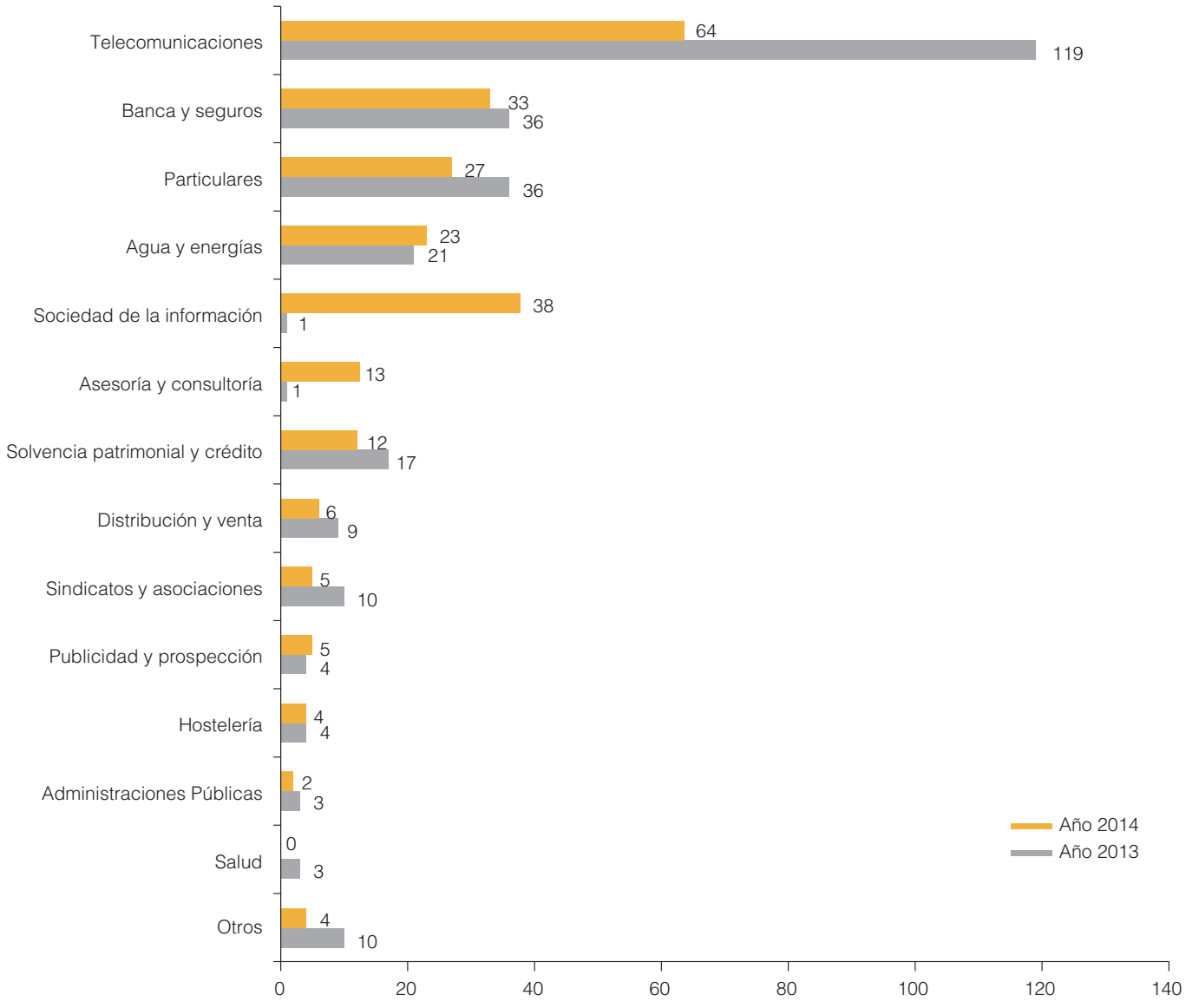
<Índice>

EVOLUCIÓN DEL SENTIDO DEL FALLO EN PORCENTAJES (2003-2014)



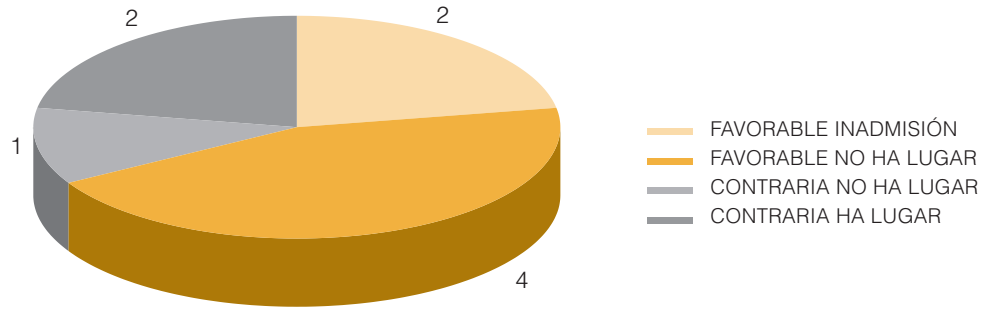
2

COMPARATIVA POR SECTOR DEL RECURRENTE (2013-2014)



<Índice>

SENTENCIAS DE TRIBUNAL SUPREMO EN 2014



3 ATENCIÓN AL CIUDADANO

CONSULTAS TOTALES PLANTEADAS ANTE EL ÁREA DE ATENCIÓN AL CIUDADANO

	Atención telefónica	Atención presencial	Atención por escrito	Atención por sede electrónica	Total	Consultas con respuesta automática
Año 2012	97.162	4.257	202	10.312	111.933	
Año 2013	92.942	3.817	668	4.637	102.064	105.092*
Año 2014	89.868	3.361	592	5.703	99.524	97.854*
% de incremento	–3,31	–11,95	–11,38	22,99	–2,49	–6,89

* Esta cifra refleja el número de accesos a la sección Preguntas más frecuentes de la Sede electrónica.

COMPARATIVA DE ACCESOS A LA PÁGINA WEB

AÑO	2012	2013	2014
Accesos web	4.096.765	4.985.648	**5.706.488**
Promedio diario	5.646	6.842	**7.816**

<Índice>

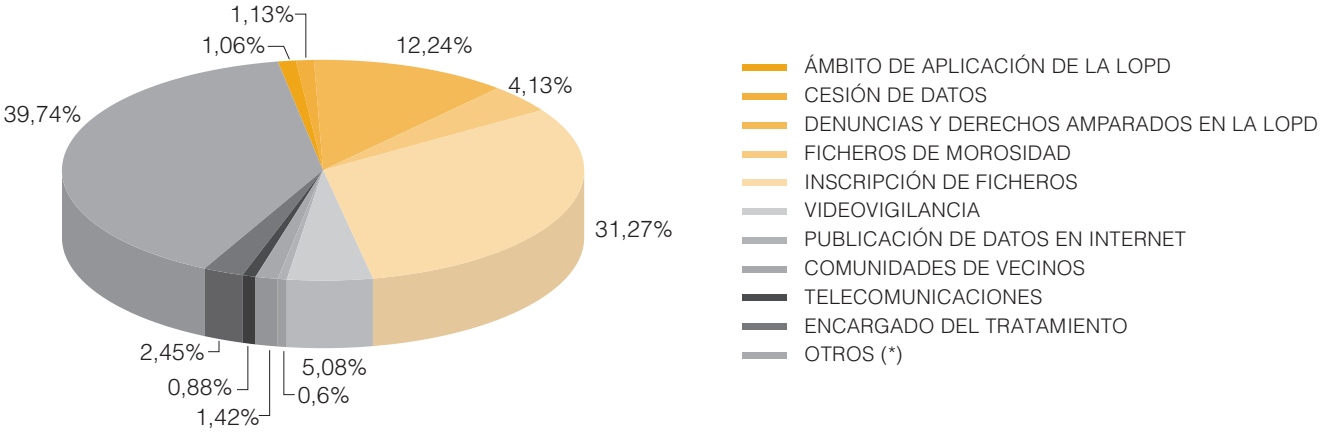
EL USO DE LA SEDE ELECTRÓNICA EN CIFRAS

	2014
Accesos web	5.706.488
Documentos presentados registro electrónico	669
Denuncias	5.825
Reclamaciones de tutela	573
Consultas de respuesta automática	97.854
Nuevas consultas de ciudadanos	5.008
NOTA. Notificación de ficheros a la Agencia	316.904
Solicitud de copias de contenido de ficheros	10.327
Test Evalúa Seguridad LOPD	12.207
DISPONE	4.876
Consulta y/o descarga de la Guía de seguridad	71.252
Descarga del modelo de documento de seguridad	139.638
Guía para el ciudadano	272.140
Guía del responsable de ficheros	90.462
Guía de videovigilancia	107.985
Guía de relaciones laborales	310.548
Guía para clientes que contraten servicios de Cloud computing	264.974
Orientaciones para prestadores de servicios de Cloud computing	61.637
Guía sobre el uso de las cookies	390.460
Guía RFID	160.351
Guía para una Evaluación de Impacto en la Protección de Datos personales	152.821

3

ANÁLISIS DE LAS CONSULTAS POR TEMAS

TEMAS	%
Ámbito de aplicación de la LOPD	1,06
Cesión de datos	1,13
Denuncias y derechos amparados en la LOPD	12,24
Ficheros de morosidad	4,13
Inscripción de ficheros	31,27
Videovigilancia	5,08
Publicación de datos en internet	0,6
Comunidades de vecinos	1,42
Telecomunicaciones	0,88
Encargado del tratamiento	2,45
Otros*	39,74

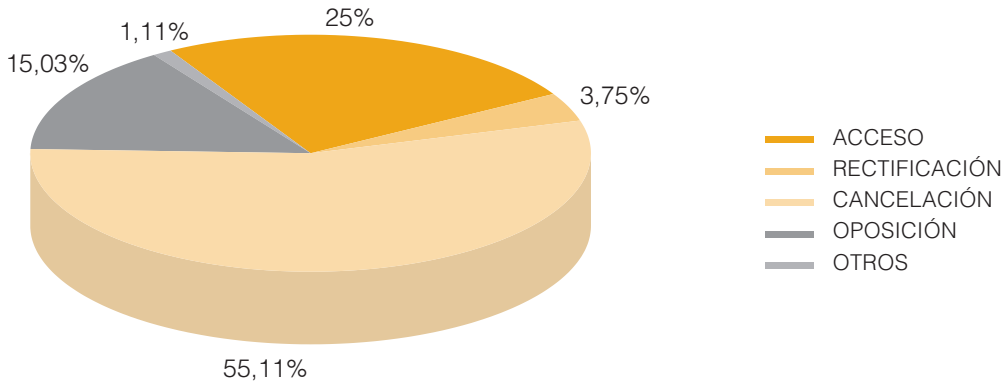


* Este apartado incluye temas como medidas de seguridad e información general sobre la LOPD y la Agencia, entre otras materias.

<Índice>

ANÁLISIS DE LAS CONSULTAS SOBRE DERECHOS ARCO

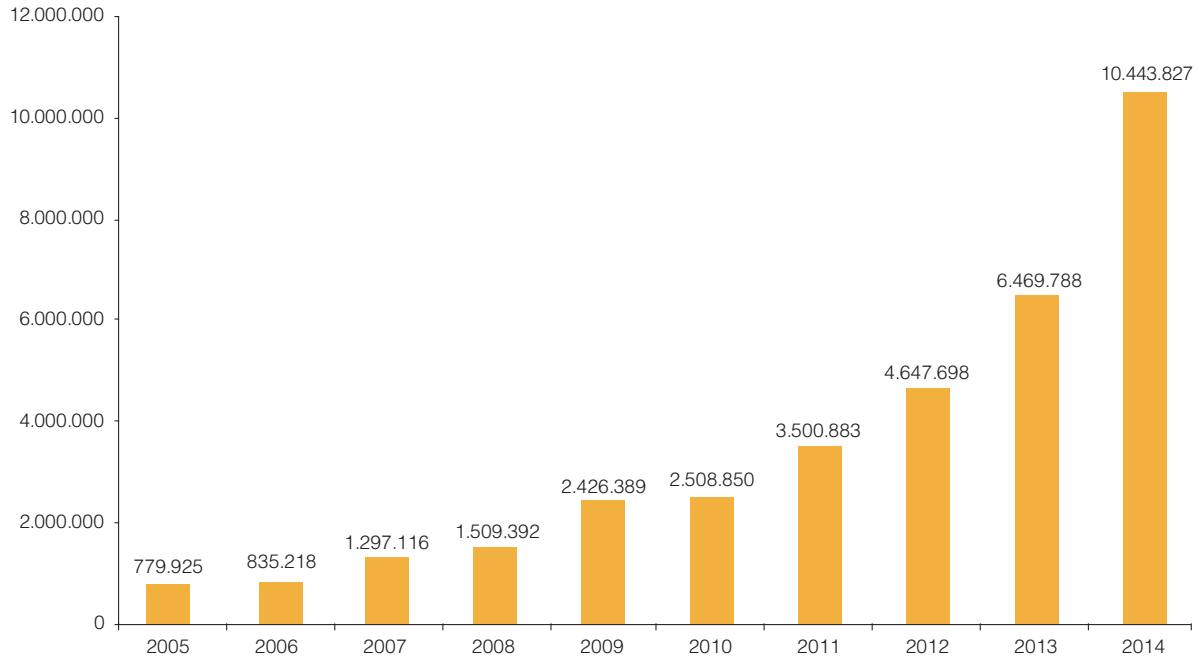
DERECHOS	%
Acceso	25,00
Rectificación	3,75
Cancelación	55,11
Oposición	15,03
Otros	1,11



4 REGISTRO GENERAL DE PROTECCIÓN DE DATOS

DERECHO DE CONSULTA AL REGISTRO

Titularidad	2013	2014
Privada	3.409.270	4.484.549
Pública	3.060.518	5.959.278
TOTAL	**6.469.788**	**10.443.827**

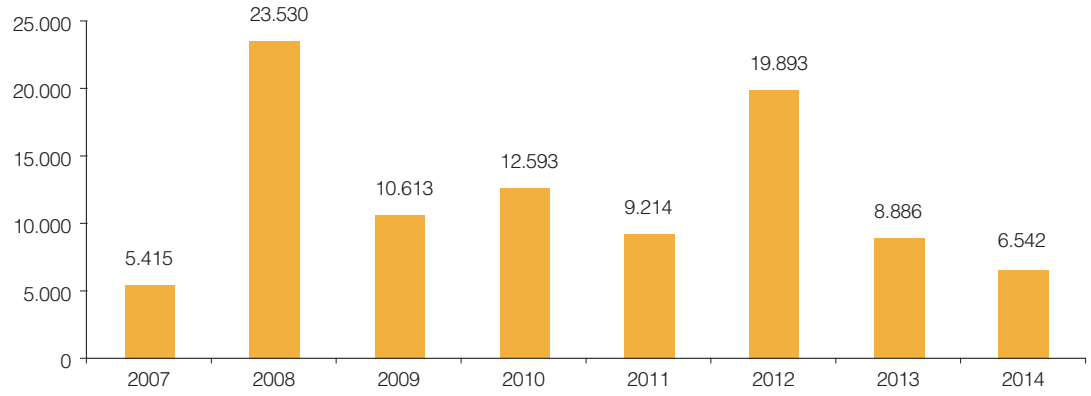


<Índice>

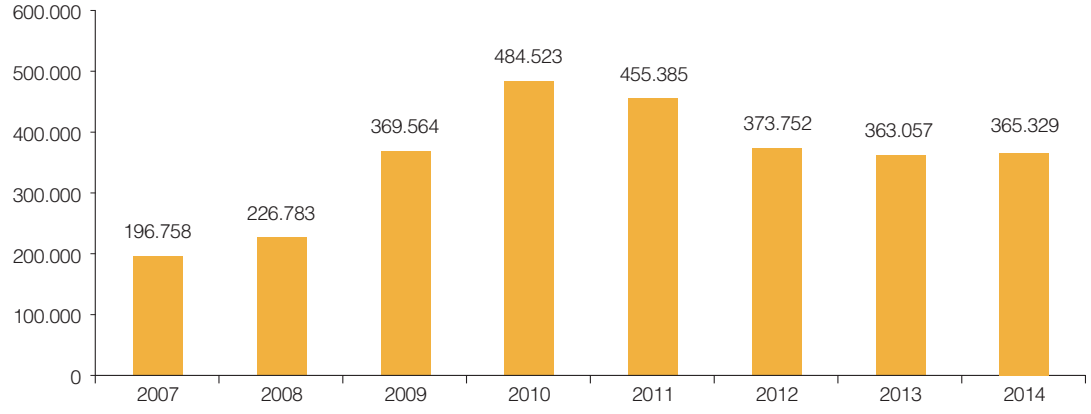
EVOLUCIÓN DE LA INSCRIPCIÓN DE FICHEROS EN EL RGPD

A 31 de diciembre	2007	2008	2009	2010	2011	2012	2013	2014
Titularidad Pública	61.553	85.083	95.696	108.289	117.503	137.396	146.282	**152.824**
Titularidad Privada	955.713	1.182.496	1.552.060	2.036.583	2.491.968	2.865.720	3.228.777	**3.594.106**
T O T A L	**1.017.266**	**1.267.579**	**1.647.756**	**2.144.872**	**2.609.471**	**3.003.116**	**3.375.059**	**3.746.930**

INCREMENTO ANUAL DE FICHEROS DE TITULARIDAD PÚBLICA



INCREMENTO ANUAL DE FICHEROS DE TITULARIDAD PRIVADA



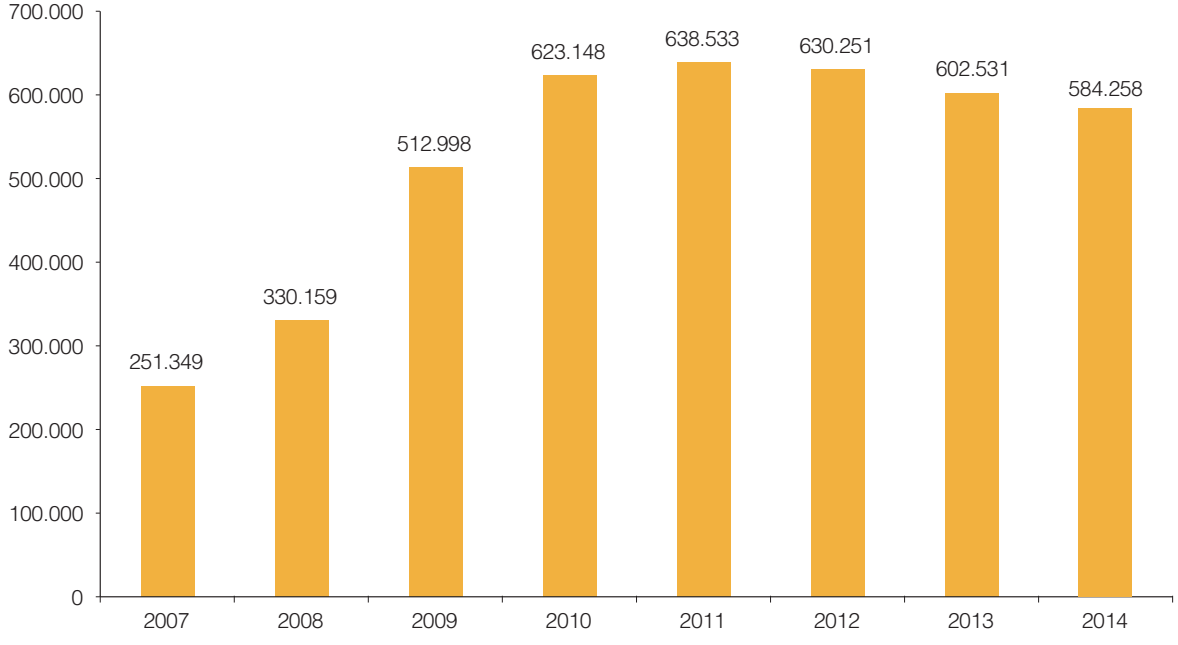
<Índice>

4

OPERACIONES DE INSCRIPCIÓN

	2013	2014	% Variación 2013-2014	Media diaria en 2013	Media diaria en 2014
Operaciones de inscripción	602.531	584.258	–3	2.511	2.434
Total de ficheros inscritos	3.375.059	3.746.930	+ 11	1.550	1.549

EVOLUCIÓN ANUAL DE LAS OPERACIONES DE INSCRIPCIÓN



<Índice>

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2014	TOTAL	2014	TOTAL
Comunidad Autónoma de Andalucía	**34.991**	**185.091**	**85.530**	**561.011**
Almería	3.831	17.498	9.488	56.112
Cádiz	5.162	23.141	14.415	69.595
Córdoba	3.152	17.192	7.749	52.689
Granada	4.670	24.877	11.327	79.669
Huelva	1.194	8.020	2.879	23.703
Jaén	2.732	14.163	6.608	48.088
Málaga	7.517	42.278	18.315	124.005
Sevilla	6.768	38.697	14.749	107.150
Comunidad Autónoma de Aragón	**5.532**	**43.138**	**11.705**	**107.200**
Huesca	914	8.249	1.819	19.733
Teruel	429	3.824	1.028	10.148
Zaragoza	4.192	31.131	8.858	77.319
Comunidad Autónoma del Principado de Asturias	**6.801**	**38.824**	**16.261**	**116.580**
Comunidad Autónoma de Canarias	**7.027**	**39.280**	**16.527**	**128.287**
Las Palmas	3.426	18.366	8.303	61.408
Santa Cruz de Tenerife	3.605	20.989	8.224	66.879
Comunidad Autónoma de Cantabria	**2.963**	**15.230**	**5.944**	**39.630**
Comunidad Autónoma de Castilla y León	**9.557**	**63.793**	**24.031**	**176.184**
Ávila	789	4.196	2.029	10.436
Burgos	1.023	10.120	2.424	24.666
León	1.646	12.178	3.848	33.204
Palencia	822	4.695	2.014	13.645
Salamanca	1.085	7.857	2.419	21.300
Segovia	1.434	5.244	4.300	15.973
Soria	377	2.721	811	7.633
Valladolid	1.898	13.091	4.998	36.942
Zamora	490	3.838	1.188	12.385

4

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2014	TOTAL	2014	TOTAL
Comunidad Autónoma de Castilla-La Mancha	**7.054**	**46.212**	**17.770**	**137.633**
Albacete	1.508	11.755	3.771	37.068
Ciudad Real	1.906	10.660	4.982	32.493
Cuenca	605	4.542	1.395	12.514
Guadalajara	789	5.085	1.871	13.458
Toledo	2.254	14.251	5.751	42.100
Comunidad Autónoma de Cataluña	**28.114**	**234.338**	**70.823**	**617.377**
Barcelona	21.377	174.318	53.052	452.683
Girona	2.717	27.798	6.977	75.727
Lleida	1.262	11.994	3.180	30.874
Tarragona	2.772	20.610	7.614	58.093
Comunidad de Madrid	**36.771**	**213.138**	**85.464**	**547.637**
Comunitat Valenciana	**24.143**	**152.041**	**56.941**	**404.802**
Alicante/Alacant	8.865	53.210	21.085	135.249
Castellón/Castelló	2.390	17.507	5.267	49.301
Valencia/Vàlencia	12.893	81.494	30.589	220.252
Comunidad Autónoma de Extremadura	**3.813**	**22.391**	**8.869**	**65.583**
Badajoz	2.379	14.013	5.650	40.884
Cáceres	1.437	8.409	3.219	24.699
Comunidad Autónoma de Galicia	**13.515**	**90.037**	**30.385**	**260.251**
A Coruña	5.967	39.501	13.723	113.310
Lugo	1.975	11.597	4.527	32.000
Ourense	1.222	9.649	2.754	26.372
Pontevedra	4.370	29.521	9.381	88.569
Comunidad Autónoma de las Illes Balears	**5.236**	**28.944**	**14.854**	**100.932**
Comunidad Foral de Navarra	**2.162**	**14.221**	**5.670**	**41.855**
Comunidad Autónoma del País Vasco	**8.208**	**52.844**	**20.325**	**143.428**
Araba/Álava	1.155	7.308	2.381	18.937
Gipuzkoa	2.865	16.779	8.288	49.090
Bizkaia	4.197	28.846	9.656	75.401

<Índice>

DISTRIBUCIÓN TERRITORIAL DE FICHEROS	RESPONSABLES		FICHEROS	
	2014	TOTAL	2014	TOTAL
Comunidad Autónoma de La Rioja	1.191	11.279	2.803	29.010
Comunidad Autónoma de la Región de Murcia	6.772	39.918	16.511	109.746
Ciudad Autónoma de Ceuta	221	857	528	2.273
Ciudad Autónoma de Melilla	375	896	900	4.433

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS	2014	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	**5.598**	83.594
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	**39.950**	410.773
Datos de carácter identificativo	**416.816**	3.594.106
Datos de características personales	**181.917**	1.614.984
Datos de circunstancias sociales	**121.170**	945.851
Datos académicos y profesionales	**103.006**	913.469
Detalles de empleo y carrera administrativa	**112.191**	1.111.099
Datos de información comercial	**123.176**	1.015.395
Datos económico-financieros	**215.933**	2.041.243
Datos de transacciones	**175.073**	1.527.600
Otros tipos de datos	**20.897**	154.108

4

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD	2014	TOTAL	% VARIACIÓN 2014/TOTAL*
Gestión de clientes, contable, fiscal y administrativa	**215.373**	2.122.741	+ 10,15
Recursos humanos	**86.797**	811.720	+ 10,69
Gestión de nóminas	**59.480**	601.312	+ 9,89
Publicidad y prospección comercial	**51.065**	310.154	+ 16,46
Prevención de riesgos laborales	**42.707**	314.292	+ 13,59
Videovigilancia	**38.423**	204.484	+ 18,79
Comercio electrónico	**25.381**	100.524	+ 25,25
Gestión y control sanitario	**17.975**	146.273	+ 12,29
Historial clínico	**13.253**	103.266	+ 12,83
Seguridad y control de acceso a edificios	**9.320**	55.877	+ 16,68
Análisis de perfiles	**8.730**	49.736	+ 17,55
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales	**5.358**	53.399	+ 10,03
Educación	**4.390**	44.398	+ 9,89
Cumplimiento/incumplimiento de obligaciones dinerarias	**4.220**	47.948	+ 8,80
Fines estadísticos, históricos o científicos	**4.048**	89.447	+ 4,53
Servicios económicos-financieros y seguros	**3.706**	68.955	+ 5,37
Seguridad privada	**3.625**	23.314	+ 15,55
Prestación de servicios de comunicaciones electrónicas	**3.438**	21.534	+ 15,97
Guías/repertorios de servicios de comunicaciones electrónicas	**2.672**	15.553	+ 17,18
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	**1.681**	19.353	+ 8,69
Gestión de asistencia social	**1.301**	14.495	+ 8,98
Investigación epidemiológica y actividades análogas	**906**	9.276	+ 9,77
Prestación de servicios de solvencia patrimonial y crédito	**635**	8.434	+ 7,53
Prestación de servicios de certificación electrónica	**489**	3.328	+ 14,69
Otras finalidades	**77.791**	574.745	+ 13,53

* Porcentaje de crecimiento por finalidad declarada.

<Índice>

INSCRIPCIÓN DE TITULARIDAD PRIVADA

DISTRIBUCIÓN DE FICHEROS SEGÚN EL SECTOR DE ACTIVIDAD	2014	TOTAL	% VARIACIÓN 2014/TOTAL
Comunidades de propietarios	**54.753**	451.403	+ 12,13
Comercio	**50.756**	426.446	+ 11,90
Sanidad	**35.694**	270.072	+ 13,22
Turismo y hostelería	**24.149**	175.542	+ 13,76
Contabilidad, auditoría y asesoría fiscal	**12.318**	154.770	+ 7,96
Educación	**10.061**	88.187	+ 11,41
Actividades inmobiliarias	**9.909**	108.792	+ 9,11
Construcción	**9.688**	131.433	+ 7,37
Actividades jurídicas, notarios y registradores	**8.868**	87.449	+ 10,14
Asociaciones y clubes	**8.472**	77.793	+ 10,89
Transporte	**8.255**	80.030	+ 10,31
Servicios informáticos	**5.068**	51.903	+ 9,76
Activ. de organizaciones empresariales, profesionales y patronales	**4.763**	18.913	+ 25,18
Industria química y farmacéutica	**4.457**	56.296	+ 7,92
Comercio y servicios electrónicos	**4.178**	20.099	+ 20,79
Agricultura, ganadería, explotación forestal, caza, pesca	**4.009**	39.722	+ 10,09
Actividades diversas de servicios personales	**4.005**	35.826	+ 11,18
Actividades relacionadas con los productos alimenticios, bebidas y tabacos	**3.999**	45.239	+ 8,84
Maquinaria y medios de transporte	**3.027**	45.099	+ 6,71
Seguros privados	**2.518**	32.666	+ 7,71
Actividades de servicios sociales	**2.289**	28.502	+ 8,03
Producción de bienes de consumo	**1.924**	27.577	+ 6,98
Sector energético	**1.738**	23.463	+ 7,41
Actividades políticas, sindicales o religiosas	**1.553**	19.610	+ 7,92
Servicios de telecomunicaciones	**1.484**	15.822	+ 9,38
Actividades relacionadas con los juegos de azar y apuestas	**1.042**	9.402	+ 11,08
Publicidad directa	**986**	11.889	+ 8,29
Seguridad	**733**	8.408	+ 8,72
Entidades bancarias y financieras	**676**	13.377	+ 5,05
Organización de ferias, exhibiciones, congresos y otras activ. relac.	**522**	4.457	+ 11,71
Investigación y desarrollo (I+D)	**457**	4.730	+ 9,66
Inspección técnica de vehículos y otros análisis técnicos	**351**	3.947	+ 8,89
Selección de personal	**275**	4.710	+ 5,84
Actividades postales y de correo	**225**	3.188	+ 7,06
Solvencia patrimonial y crédito	**61**	1.112	+ 5,49
Mutualidades colaboradoras de los organismos de la seguridad social	**31**	849	+ 3,65
Otras actividades	**133.522**	983.199	+ 13,58

<Índice>

4

INSCRIPCIÓN DE TITULARIDAD PÚBLICA

DISTRIBUCIÓN DE FICHEROS POR TIPO DE ADMINISTRACIÓN	2014	TOTAL
Administración General	636	8.040
Administración CC.AA.	1.252	29.432
Administración Local	7.454	88.051
Otras personas jurídico-públicas	611	27.301
TOTAL	**9.953**	**152.824**

DISTRIBUCIÓN DE FICHEROS DE LA ADMINISTRACIÓN GENERAL

	FICHEROS
Presidencia del Gobierno	8
Ministerio de Asuntos Exteriores y de Cooperación	541
Ministerio de Justicia	148
Ministerio de Defensa	1.812
Ministerio de Hacienda y Administraciones Públicas	1.000
Ministerio del Interior	224
Ministerio de Fomento	555
Ministerio de Educación, Cultura y Deporte	282
Ministerio de Empleo y Seguridad Social	1.673
Ministerio de Industria, Energía y Turismo	220
Ministerio de Agricultura, Alimentación y Medio Ambiente	447
Ministerio de la Presidencia	57
Ministerio de Economía y Competitividad	503
Ministerio de Sanidad, Servicios Sociales e Igualdad	570
TOTAL	**8.040**

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA-CC.AA.

	2014	FICHEROS
Comunidad Autónoma de Andalucía	92	1.952
Comunidad Autónoma de Aragón	43	376
Comunidad Autónoma del Principado de Asturias	26	518
Comunidad Autónoma de Canarias	11	436
Comunidad Autónoma de Cantabria	4	229
Comunidad Autónoma de Castilla y León	60	936
Comunidad Autónoma de Castilla-La Mancha	16	817
Comunidad Autónoma de Cataluña	163	10.080
Comunidad de Madrid	301	9.817
Comunitat Valenciana	9	571
Comunidad Autónoma de Extremadura	71	504
Comunidad Autónoma de Galicia	16	325
Comunidad Autónoma de las Illes Balears	19	564
Comunidad Foral de Navarra	4	171
Comunidad Autónoma del País Vasco	374	1.341
Comunidad Autónoma de La Rioja	26	230
Comunidad Autónoma de la Región de Murcia	15	438
Ciudad Autónoma de Ceuta	2	38
Ciudad Autónoma de Melilla	0	89
TOTAL	**1.252**	**29.432**

4

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA-ADMINISTRACIÓN LOCAL

	ENTIDADES	FICHEROS
Comunidad Autónoma de Andalucía	**864**	**10.756**
Almería	112	1.263
Cádiz	49	772
Córdoba	94	943
Granada	194	1.567
Huelva	88	1.274
Jaén	92	808
Málaga	109	2.157
Sevilla	126	1.972
Comunidad Autónoma de Aragón	**584**	**5.734**
Huesca	198	1.770
Teruel	77	536
Zaragoza	309	3.428
Comunidad Autónoma del Principado de Asturias	**91**	**1.497**
Comunidad Autónoma de Canarias	**115**	**1.812**
Las Palmas	51	855
Santa Cruz de Tenerife	64	957
Comunidad Autónoma de Cantabria	**68**	**891**
Comunidad Autónoma de Castilla y León	**1.190**	**10.325**
Ávila	95	1.078
Burgos	344	2.560
León	208	1.357
Palencia	121	1.274
Salamanca	92	551
Segovia	63	720
Soria	17	87
Valladolid	207	2.456
Zamora	43	242

	ENTIDADES	FICHEROS
Comunidad Autónoma de Castilla-La Mancha	**489**	**7.207**
Albacete	101	3.479
Ciudad Real	110	874
Cuenca	121	1.025
Guadalajara	31	442
Toledo	126	1.387
Comunidad Autónoma de Cataluña	**1.057**	**12.409**
Barcelona	440	5.666
Girona	227	2.853
Lleida	217	2.111
Tarragona	174	1.779
Comunidad de Madrid	**235**	**4.678**
Comunitat Valenciana	**507**	**7.043**
Alicante/Alacant	162	2.355
Castellón/Castelló	100	1.055
Valencia/València	246	3.633
Comunidad Autónoma de Extremadura	**315**	**7.748**
Badajoz	192	6.031
Cáceres	123	1.717
Comunidad Autónoma de Galicia	**329**	**4.369**
A Coruña	100	1.523
Lugo	69	777
Ourense	90	1.032
Pontevedra	70	1.037
Comunidad Autónoma de las Illes Balears	**86**	**1.579**
Comunidad Foral de Navarra	**247**	**2.649**
Comunidad Autónoma del País Vasco	**359**	**7.664**
Araba/Álava	62	741
Gipuzkoa	128	2.240
Bizkaia	169	4.683
Comunidad Autónoma de La Rioja	**43**	**407**
Comunidad Autónoma de la Región de Murcia	**56**	**1.282**

<Índice>

DISTRIBUCIÓN DE FICHEROS DE TIRULARIDAD PÚBLICA. OTRAS PERSONAS JURÍDICO-PÚBLICAS

	TOTAL
Cámaras Oficiales de Comercio e Industria	481
Notariado	8.110
Universidades	1.482
Colegios Profesionales	2.649
Otros	14.579
TOTAL	**27.301**

DISTRIBUCIÓN DE FICHEROS SEGÚN TIPOS DE DATOS

	2014	TOTAL
Datos especialmente protegidos (ideología, creencias, religión y afiliación sindical)	373	19.316
Otros datos especialmente protegidos (origen racial, salud y vida sexual)	1.705	37.961
Datos relativos a infracciones	1.737	26.438
Datos de carácter identificativo	9.953	152.824
Datos de características personales	4.857	78.874
Datos de circunstancias sociales	3.613	41.699
Datos académicos y profesionales	3.010	50.069
Detalles de empleo y carrera administrativa	2.508	44.902
Datos de información comercial	1.943	19.446
Datos económico-financieros	4.572	67.160
Datos de transacciones	1.984	29.325
Otros tipos de datos	1.326	22.529

<Índice>

DISTRIBUCIÓN DE FICHEROS CON DATOS SENSIBLES

	2014	TOTAL
Datos especialmente protegidos	**373**	**19.316**
Ideología	113	9.367
Creencias	61	8.571
Religión	123	8.949
Afiliación Sindical	196	17.835
Otros datos especialmente protegidos	**1.705**	**37.961**
Origen Racial	251	11.918
Salud	1.697	37.786
Vida Sexual	119	9.639
Datos relativos a infracciones	**1.737**	**26.438**
Infracciones Penales	677	17.840
Infracciones Administrativas	1.654	25.572

4

DISTRIBUCIÓN DE FICHEROS SEGÚN SU FINALIDAD

	2014	TOTAL	% 2014/TOTAL
Procedimiento administrativo	3.031	50.085	+6,05
Gestión contable, fiscal y administrativa	1.045	22.321	+4,68
Recursos humanos	1.038	26.933	+3,85
Educación y cultura	1.036	16.391	+6,32
Fines históricos, estadísticos o científicos	765	19.999	+3,83
Servicios sociales	661	9.881	+6,69
Gestión sancionadora	610	5.765	+10,58
Gestión de nómina	463	13.058	+3,55
Hacienda pública y gestión de administración tributaria	458	10.510	+4,36
Publicaciones	382	2.657	+14,38
Videovigilancia	375	2.632	+14,25
Gestión económica-financiera pública	365	6.814	+5,36
Seguridad pública y defensa	359	3.958	+9,07
Función estadística pública	345	12.747	+2,71
Prevención de riesgos laborales	328	3.496	+9,38
Seguridad y control de acceso a edificios	273	3.770	+7,24
Actuaciones de fuerzas y cuerpos de seguridad con fines policiales	262	2.560	+10,23
Padrón de habitantes	259	6.619	+3,91
Trabajo y gestión de empleo	244	5.688	+4,29
Gestión y control sanitario	157	4.043	+3,88
Justicia	95	10.619	+0,89
Investigación epidemiológica y actividades análogas	86	1.677	+5,13
Historial clínico	69	2.421	+2,85
Prestación de servicios de certificación electrónica	52	1.698	+3,06
Gestión de censo promocional	30	1.020	+2,94
Otras finalidades	4.106	42.785	+9,60

RESOLUCIONES DE AUTORIZACIÓN

		2000–2006	07	08	09	10	11	12	13	2014	Total Aut.
Estados Unidos 377	EEUU	83	10	31	28	25	40	62	47	51	377
Iberoamérica 456	Panamá	2	–	–	–	–	–	–	1	3	6
	Colombia	5	9	4	12	22	23	17	21	23	136
	Chile	8	9	1	8	9	7	1	–	–	43
	Uruguay	2	1	4	3	13	–	2	–	–	25
	Perú	4	5	4	19	20	30	23	23	5	133
	Guatemala	1	–	1	1	–	–	2	1	–	6
	Paraguay	1	1	4	4	1	4	2	–	–	17
	Brasil	–	1	3	–	1	2	2	3	1	13
	El Salvador	–	1	–	–	–	–	–	–	–	1
	Costa Rica	–	1	1	–	1	1	2	1	–	7
	Nicaragua	–	1	–	–	–	–	–	–	–	1
	México	–	–	3	8	20	12	14	7	2	66
	Ecuador	–	–	–	–	1	–	–	–	–	1
	Venezuela	–	–	–	–	–	–	–	–	1	1
India 232	India	7	2	30	28	14	29	27	42	53	232
Otros países 282	Marruecos	7	1	3	8	7	4	10	13	9	62
	Singapur	2	2	–	–	1	2	4	1	6	18
	Japón	1	1	–	1	1	3	4	7	7	25
	Malasia	2	1	–	3	–	–	2	1	5	14
	Tailandia	1	1	–	–	–	–	1	–	–	3
	Filipinas	3	1	5	4	3	5	9	8	5	43
	China	1	1	3	3	1	14	4	6	–	33
	Hong Kong	1	–	–	1	1	–	1	2	–	6
	Egipto	–	1	–	–	–	–	1	1	–	3
	Nigeria	–	1	–	–	–	–	–	–	–	1
	Túnez	–	1	–	–	2	–	3	–	–	6
	Sudáfrica	–	–	3	–	–	–	3	–	1	7
	Australia	–	1	–	7	–	–	3	4	3	18
	Canadá	–	1	–	–	–	–	1	–	2	4
	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	–	1	3
	Croacia	–	–	–	–	–	–	1	–	–	1
	Turquía	–	–	–	–	–	–	1	–	–	1
	Ucrania	–	–	–	–	–	–	1	–	–	1
	Bermudas	–	–	–	–	1	–	1	–	–	2
	Nueva Zelanda	–	–	–	–	–	–	1	–	1	2
	Rep. de Corea	–	–	–	–	–	–	1	–	1	2
	Federación Rusa	–	–	–	–	–	–	1	1	–	2
	Emiratos Árabes	–	–	–	–	–	–	–	1	–	1
Internacional 17	Internacional*	–	–	–	–	3	1	3	8	2	17
	Solicitudes presentadas	187	127	137	166	197	201	224	192	187	1.618
	Archivadas	52	68	42	24	31	16	52	15	26	326
	Total Autorizaciones	131	43	103	128	155	175	177	170	150	1.232

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

4

FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES SEGÚN TITULARIDAD

	FICHEROS
Titularidad Privada	**14.751**
Titularidad Pública	**8.348**
TOTAL	23.099

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

	2010	2011	2012	2013	2014
2001/497/CE[1]	80	112	167	195	**226**
2002/16/CE[2]- 2010/87/UE[3]	475	619	735	861	**966**
BCR	–	1	8	17	**23**
Cláusulas Encargado-Subencargado[4]	–	–	2	9	**16**
Contrato ad hoc	–	–	–	–	**1**

[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.

[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 el 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] RESOLUCIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS de 16 de octubre de 2012.

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

	2012	2013	2014	TOTAL
Ficheros	1	1.561	1.625	3.187
Responsables	1	454	437	892

TRANSFERENCIAS INTERNACIONALES DE DATOS AMPARADAS EN LA AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES BASADAS EN CONTRATO AD HOC

	2014
Ficheros	**59**
Responsables	**14**

ACTUACIONES COMO AUTORIDAD CORREVISORA DE NORMAS CORPORATIVAS VINCULANTES (BCR)

	2010	2011	2012	2013	2014	TOTAL
Revisión BCR	1	4	7	3	**7**	**22**

EVOLUCIÓN DE LA INSCRIPCIÓN DE LOS FICHEROS DE VIDEOVIGILANCIA

AÑO DE INSCRIPCIÓN	TITULARIDAD PRIVADA*	TITULARIDAD PÚBLICA*
1994 - 2007	5.419	104
2008	8.457	154
2009	20.354	260
2010	30.290	760
2011	34.757	472
2012	34.383	543
2013	37.477	472
2014	38.824	489
TOTAL	**209.961**	**3.254**

* 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. Por ejemplo, ficheros cuya finalidad tipificada es la de seguridad privada y su denominación es la de «videovigilancia» o «CCTV».

4

FICHEROS DE VIDEOVIGILANCIA DE TITULARIDAD PRIVADA

SECTOR DE ACTIVIDAD PRINCIPAL	2013	2014	% VARIACIÓN 2013-2014
Comercio	41.599	49.889	+19,93
Turismo y hostelería	20.672	24.830	+20,11
Comunidades de propietarios	12.831	16.106	+25,52
Sanidad	9.230	11.258	+21,97
Activ. relacionadas con los productos alimenticios, bebidas y tabacos	3.737	4.337	+16,06
Construcción	3.679	4.265	+15,93
Transporte	3.000	3.705	+23,50
Industria química y farmacéutica	3.047	3.490	+14,54
Educación	2.289	2.747	+20,01
Actividades inmobiliarias	2.215	2.656	+19,91
Maquinaria y medios de transporte	1.930	2.278	+18,03
Servicios informáticos	1.889	2.149	+13,76
Contabilidad, auditoría y asesoría fiscal	1.586	1.982	+24,97
Actividades relacionadas con los juegos de azar y apuestas	1.691	1.899	+12,30
Agricultura, ganadería, explotación forestal, caza, pesca	1.489	1.871	+25,65
Asociaciones y clubes	1.495	1.821	+21,81
Sector energético	1.582	1.780	+12,52
Seguridad	1.532	1.672	+9,14
Producción de bienes de consumo	1.297	1.482	+14,26
Actividades diversas de servicios personales	1.042	1.247	+19,67
Servicios de telecomunicaciones	1.055	1.174	+11,28
Actividades de servicios sociales	942	1.096	+16,35
Actividades jurídicas, notarios y registradores	804	977	+21,52
Comercio y servicios electrónicos	719	879	+22,25
Entidades bancarias y financieras	518	674	+30,12
Activ. de organizaciones empresariales, profesionales y patronales	345	584	+69,28
Seguros privados	387	461	+19,12
Actividades políticas, sindicales o religiosas	335	393	+17,31
Inspección técnica de vehículos y otros análisis técnicos	232	263	+13,36
Publicidad directa	182	215	+18,13
Organización de ferias, exhibiciones, congresos y otras activ. relac.	163	185	+13,50
Investigación y desarrollo (I+D)	153	170	+11,11
Activ. postales y de correo (oper. postales, serv. post., transport.)	112	129	+15,18
Selección de personal	44	47	+6,82
Mutualidades colaboradoras de los organismos de la seguridad social	24	25	+4,17
Solvencia patrimonial y crédito	15	15	+0,00
Otras actividades	49.634	61.210	+23,33
TOTAL	**173.496**	**209.961**	**+21,02**

<Índice>

PRESENCIA INTERNACIONAL DE LA AEPD 5

Reunión	Fecha	Lugar
Sesiones Plenarias del Grupo de Trabajo del Artículo 29 (GT29)	26 y 27 febrero 9 y 10 abril 3 y 4 junio 16 y 17 septiembre 25 y 26 noviembre	Bruselas (Bélgica)
Reuniones de subgrupos en la Comisión Europea		
Futuro de la privacidad (FoP)	3 y 4 abril 15 y 24 julio 8 octubre 14 noviembre	Bruselas (Bélgica)
Tecnología (TS)	15 y 16 enero 18-20 marzo 13 y 14 mayo 8 y 9 julio 21 y 22 octubre	Bruselas (Bélgica)/ Ispra (Italia)
Borders, Travels & Law Enforcement (BTLE)	14 enero 20 marzo 4 y 5 noviembre	Bruselas (Bélgica)
E-Government	5 y 6 febrero	Bruselas (Bélgica)
Otras reuniones		
Grupo DAPIX	9, 21 y 27 enero 5, 19 y 20 feb 11, 12 y 24 marzo 1 abril 11 y 12 junio 9-11 julio 12 y 30 septiembre 1, 21 y 22 octubre 20 y 21 noviembre	Bruselas (Bélgica)
Second Identities at the borders Seminar (Biometrics Institute)	29 abril	Bruselas (Bélgica)
Autoridades Comunes de Control		
EUROPOL	19 marzo 16 junio 24 noviembre Inspección anual a Europol: 4-7 marzo Auditoría datos de agencias de inteligencia: 23-25 septiembre Plenario Europol: 1 y 2 octubre	Bruselas (Bélgica) La Haya (P. Bajos) Bruselas (Bélgica)

<Índice>

5

Reunión	Fecha	Lugar
EURODAC	7 y 8 mayo 27-29 octubre	
Grupos de Supervisión Coordinada de los sistemas VIS, SIS y EURODAC	7 y 8 mayo 27-29 octubre	
EUROJUST	19 y 20 junio	La Haya (P. Bajos)
Consejo de Europa		
Reunión TC-Y Reunión Law enforcement	27 y 28 mayo 18 junio	Estrasburgo (Francia)
Grupos de trabajo sectoriales		
Grupo de Telecomunicaciones de Berlín	4-6 mayo	Skopje (Macedonia)
	13-15 octubre	Berlín (Alemania)
Grupo de Expertos en Retención de Datos en Telecomunicaciones	14 marzo	Bruselas (Bélgica)
GT Quiebras de seguridad transfronteriza (Data Breaches)	11 marzo	Bruselas (Bélgica)
	11-13 junio	Ispra (Italia)
	22-23 octubre	
Grupo de expertos India	5 febrero	Bruselas (Bélgica)
Conferencias Internacionales		
Conferencia de primavera de Autoridades Europeas de Protección de Datos	4 junio	Estrasburgo (Francia)
Cooperation in Data Protection Law Enforcement	3-4 abril	Manchester (Reino Unido)
36ª Conferencia internacional de Autoridades de Protección de Datos	13-17 octubre	Mauricio
Otras Reuniones		
Reuniones con la CNIL	10-12 septiembre	París (Francia)
GOOGLE	14 y 15 enero 6 y 7 febrero 2 julio	
Internet de las Cosas (IoT)	24 julio	
Conference of the European Data Governance Forum (en colaboración con la UNESCO)	8 diciembre	
Convenio Cibercrimen	18 y 19 junio	Estrasburgo (Francia)
Annual Privacy Forum 2014	19-21 junio	Atenas (Grecia)
Privacy Risk Framework Project Workshop	19 y 20 marzo	París (Francia)
	18 noviembre	Bruselas (Bélgica)

SECRETARÍA GENERAL 6

GESTIÓN DE RECURSOS HUMANOS

		DOTACIÓN 31/12/2014	CUBIERTOS 31/12/2014
PUESTOS DE TRABAJO	Funcionarios	157	151
	Laborales	4	2
	Laborales fuera de Convenio	2	2
	Alto cargo	1	1
		164	**156**

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos 2014	6	3	22	46	2	15	3	11	2	7	12	22

	A1	A2	C1	C2
Efectivos 2014	32	46	22	51

MUJERES	**87**
HOMBRES	**69**

<Índice>

6

EVOLUCIÓN DEL PRESUPUESTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

	CRÉDITO EJERCICIO 2012 (EUROS)	CRÉDITO EJERCICIO 2013 (EUROS)	CRÉDITO EJERCICIO 2014 (EUROS)
CAPITULO I	6.346.260	6.672.660	6.672.660
CAPITULO II	5.474.130	5.024.000	5.224.000
CAPITULO III	546.740	432.450	232.450
CAPITULO VI	1.539.620	1.372.160	1.316.000
CAPITULO VIII	22.800	22.800	22.800
TOTAL	**13.929.550**	**13.524.070**	**13.467.910**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEMORIA AEPD 2014

www.agpd.es