

MEMORIA AEPD 2018

prólogo

Un año más me complace presentar la Memoria de la Agencia Española de Protección de Datos. En esta ocasión, además del análisis de las tendencias, los retos a los que se enfrenta la protección de datos y un resumen de las actividades y decisiones más relevantes, las páginas que siguen reflejan un punto de inflexión en materia de protección de datos. La aplicación el 25 de mayo de 2018 del Reglamento 2016/679 General de Protección de Datos ha supuesto un reto de enorme envergadura a varios niveles. Con anterioridad a su entrada en vigor en 2016, la AEPD aprobó un Plan estratégico con 113 medidas iniciales que contemplaban tanto ayudar a los sujetos obligados a cumplir con la nueva normativa como concienciar a los ciudadanos –en 2017 lo componían 131 y en 2018 la cifra se ha ampliado a 148–. En paralelo, la propia Agencia también comenzó a prepararse para el que ha sido uno de los mayores desafíos desde su creación. Esta Memoria, al ser anual, recoge el tránsito del anterior marco legislativo al nuevo Reglamento en todos los niveles. La estructura del texto, en consecuencia, es diferente a la de años anteriores, ya que incluye en un año natural varios marcos normativos que, aun manteniendo la misma esencia, parten de un enfoque muy diferente. A ello se ha sumado la aprobación de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales en diciembre de este año, que adapta el derecho español al Reglamento.

El nuevo Reglamento ha aportado mejoras significativas en el régimen europeo, mejorando los derechos de los ciudadanos y ampliando las vías para que aquellos que tratan datos personales puedan demostrar su cumplimiento. Se ha hecho necesario, por tanto, intensificar las labores de concienciación sin dejar de trabajar en los procedimientos abiertos y en las nuevas reclamaciones y, en paralelo, implantar un nuevo sistema de funcionamiento interno que permitiese seguir dando respuesta en esta doble vertiente.

La Agencia ha vivido una profunda reorganización de su estructura interna, impulsando a la vez la promoción de herramientas y orientaciones que faciliten la adaptación al nuevo marco por parte de responsables y encargados del tratamiento, y, en particular, las pymes. La supresión de la obligación de notificar ficheros al Registro General de Protección de Datos; la obligatoria aplicación del principio de responsabilidad proactiva; la mayor flexibilidad en el régimen de transferencias internacionales de datos; la nueva regulación de los códigos de conducta y el lanzamiento del registro de Delegados de protección de datos ha supuesto una transformación interna sustancial, además de realizar e impulsar acciones de difusión con distintos sectores empresariales, profesionales, y con las administraciones públicas. La puesta en marcha de los mecanismos de cooperación y coherencia entre las Autoridades europeas de protección de datos que exige el

Reglamento, con el desarrollo y la implantación de mecanismos colaborativos para la gestión de incidencias que pueden incumbir a varios Estados, también ha sido otra de las áreas complejas en las que la Agencia se ha involucrado.

En cuanto a las cifras anuales de gestión, las entradas recibidas han pasado de las 10.657 en 2017 a las 14.146 de este año, suponiendo un incremento de casi el 33% e incluyendo un nuevo sistema de notificación de quiebras de seguridad que ha supuesto la entrada de 547 de ellas. Y este considerable aumento no es el único que se ha producido respecto a años anteriores. Las consultas especializadas sobre el tratamiento de datos de menores se han incrementado asimismo un 75%, pasando de casi 900 en 2017 a más de 1.500; se han notificado más de 20.000 delegados de protección de datos; se han atendido más de 4.000 consultas especializadas en el Canal Informa_RGPD -presentado en 2018- y las consultas del área de Atención al ciudadano han subido hasta las casi 750.000, un incremento del 192%.

En lo relativo a la eficacia administrativa, además de haberse incrementado un 8% el número de reclamaciones resueltas con respecto a 2017 y un 18% respecto a 2016, también se ha trabajado para reducir los tiempos medios de tramitación. Así, se ha reducido un 26% y un 41% respecto a 2017 y 2016 respectivamente el número de días de resolución de los procedimientos sancionadores, unas cifras que suponen un 13% y un 28% en el caso de los procedimientos referidos al ejercicio de derechos.

Estas y otras cifras se encuentran recogidas de forma extensa en la última parte de esta Memoria agrupadas por Subdirecciones y Unidades. En este esfuerzo en dar una respuesta efectiva al ciudadano, no puede obviarse que el incremento de la carga de trabajo no ha estado acompañado por un aumento proporcional del personal de la Agencia. En 2007, una dotación de 123 personas daba respuesta a poco más de 3.000 reclamaciones recibidas. Once años después, una dotación de 187 personas debe hacer frente a más de 14.000, un incremento del 351%, y además potenciar las acciones de prevención para contribuir a una protección más eficaz de los derechos de los ciudadanos. En todo caso, también es necesario destacar que no sólo los números son indicativos del incremento de la carga de trabajo de los profesionales de esta Agencia. La atención y respuesta a cuestiones cada vez más complejas es un esfuerzo que también merece reconocimiento.

En 2018 conocimos, según datos del CIS, que a un 76.1% de los españoles le preocupa mucho o bastante la protección de sus datos personales. Como comentaba al inicio de este prólogo, la nueva legislación de protección de datos ha supuesto un enorme reto de adaptación para todos y, aun así, la normativa es sólo el marco que nos debe permitir garantizar que los ciudadanos puedan mantener el control de su propia información personal. En la Agencia Española de Protección de Datos estamos comprometidos a ello.

Mar España Martí

Directora de la Agencia Española de Protección de Datos

Índice

Memoria 2018

▲ 1. Desafíos para la privacidad	6
▲ 2. Al servicio de los ciudadanos	36
▲ 3. Ayuda efectiva para las entidades	51
▲ 4. La potestad de supervisión (Inspección)	57
▲ 5. Una estructura en permanente evolución	70
▲ 6. La necesaria cooperación institucional	73
▲ 7. Una autoridad activa en el panorama internacional	75

Anexo. La Agencia en cifras

▲ 1. Actividad global	82
▲ 2. Plan estratégico	83
▲ 3. Inspección de datos	86
▲ 4. Gabinete jurídico	98
▲ 5. Atención al ciudadano y sujetos obligados	106
▲ 6. Registro General de Protección de Datos	113
▲ 7. Transferencias internacionales de datos	114
▲ 8. Secretaría General	118
▲ 9. Presencia internacional de la AEPD	120
▲ 10. Defensor del Pueblo	123

➤ 1. Desafíos para la privacidad

1.1 Normativos

El año 2018 supuso un cambio sustancial a nivel normativo, pues el 25 de mayo fue directamente aplicable el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (en adelante RGPD o el Reglamento) y, el 6 de diciembre se publicó en el Boletín Oficial del Estado la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

El Reglamento ha actualizado el sistema europeo de garantías para la protección de datos personales con el objetivo de hacer frente a los retos de la sociedad digital.

Una sociedad digital caracterizada, entre otros, por los siguientes aspectos:

- ▲ Un incremento en la intrusión en la esfera privada de los individuos a través de la conectividad a Internet de nuestros sistemas cotidianos, desde electrodomésticos a vehículos, pasando por asistentes virtuales domésticos.
- ▲ La aplicación de técnicas de inteligencia artificial sobre los datos, yendo más allá del concepto actual de Big Data, desarrollando nuevos modelos como el Smart Data, Deep Learning, etc, con capacidad de ir más allá de mostrar resultados incluyendo la toma de decisiones.
- ▲ El intenso proceso de concentración de los prestadores de servicios de la sociedad de la información con un grupo reducido de actores en posiciones dominantes que almacenan cantidades ingentes de datos.

El modelo de negocio de estos prestadores de servicios está basado habitualmente en la oferta de servicios gratuitos monetizando la información personal de sus usuarios.

Estos retos han planteado la necesidad de conciliar el desarrollo tecnológico y la innovación garantizando los derechos de los ciudadanos europeos en un mundo de servicios globalizados, actualizando los derechos ya reconocidos en la Directiva 95/46/CE e incorporando otros nuevos adaptados al entorno digital; objetivo que ha sido abordado por el RGPD.

El primer aspecto destacable del Reglamento es la ampliación del ámbito de aplicación territorial de la norma. El Reglamento permite su aplicación a responsables de tratamiento de datos personales desde terceros países, en particular, grandes corporaciones multinacionales conforme a dos criterios: que dirijan específicamente la oferta de bienes y servicios a usuarios en la Unión Europea, sean gratuitos o no; o que las actividades de tratamiento estén relacionadas con el control de su comportamiento. En tales casos, se exige una obligación adicional como es la designación de un representante en un Estado miembro de la Unión, que colabore con las autoridades de protección de datos a la hora de comprobar el cumplimiento de la norma.

Esta previsión supone una ampliación de los criterios del Tribunal de Justicia de la Unión Europea en su Sentencia de 13 de mayo de 2014 sobre el denominado derecho al olvido en Internet. Y, al superar el criterio tradicional de vincular el ámbito de aplicación de las normas al territorio, permite garantizar los derechos de los usuarios europeos en la sociedad digital. Los principios de protección de datos del Reglamento se mantienen similares a los de la Directiva 95/46/CE, si bien reforzando alguno de ellos como el de minimización.

Pero incorpora una novedad de gran relevancia al establecer el principio de responsabilidad proactiva como obligación de los responsables de tratamiento; principio que inspira el modelo de cumplimiento previsto en el Reglamento.

El Reglamento regula en términos de igualdad las bases jurídicas que legitiman el tratamiento de los datos personales, sin primar ninguna de ellas. Aunque esta previsión estaba recogida en la Directiva 95/46/CE, el legislador nacional, al transponerla al ordenamiento jurídico interno, alteró este equilibrio primando como base jurídica general la prestación del consentimiento y recogiendo las restantes bases jurídicas como excepción a esta regla general. De este modo, la aplicación del Reglamento plantea el reto de exigir un cambio de mentalidad, tanto para los responsables del tratamiento como para las autoridades de control que, sin duda, flexibilizará las opciones de tratamiento de los datos personales.

Adicionalmente, se flexibilizan las opciones para el tratamiento de categorías especiales de datos respecto de las previsiones de la Ley orgánica 15/1999, de 13 de diciembre (LOPD).

El catálogo tradicional de derechos de protección de datos se amplía con tres novedades, como son el derecho al olvido, que incorpora una novedosa exigencia de supresión de enlaces, copias o réplicas de los datos personales cuando se hayan hecho públicos, facilitando la supresión de datos en Internet; el derecho a la limitación del tratamiento y el derecho a la portabilidad, que facilitará la transmisión por medios automatizados de los datos a nuevos responsables seleccionados por los interesados, ofreciendo a los usuarios nuevas posibilidades para cambiar de prestadores de servicios online.

Asimismo, ha potenciado la transparencia exigible a los responsables del tratamiento configurando el deber de información como un derecho de los interesados, ampliando su contenido y exigiendo que la información se facilite de forma sencilla, clara y accesible.

El abanico de novedades del Reglamento alcanza, de forma particularmente destacada, al modelo de cumplimiento y al de supervisión. Partiendo del principio de responsabilidad proactiva, el Reglamento prevé que los responsables y encargados del tratamiento apliquen medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar su cumplimiento. Medidas aplicables en función del análisis de riesgo para los derechos y libertades de los interesados, a partir de los principios de protección desde el diseño y por defecto. Y enumera dichas medidas mencionando el registro de actividades de tratamiento; las evaluaciones de impacto en la protección de datos y la obligatoriedad de designar un Delegado de protección de datos en determinadas circunstancias; la aplicación de medidas de seguridad adecuadas; la notificación de violaciones de seguridad; los códigos de conducta y los esquemas de certificación.

De este modo, el Reglamento opta por una doble estrategia de prevención y flexibilización que hace, también, necesario un cambio de mentalidad para su cumplimiento. Y es en la forma de aplicar estas medidas donde el Reglamento introduce una dimensión de flexibilidad, ya que no todas las organizaciones han de aplicar íntegramente dichas medidas, ni han de hacerlo del mismo modo, atendiendo al análisis de riesgo que deben realizar.

La aplicación del Reglamento exige un cambio de mentalidad, lo que constituye un reto no sólo para los responsables sino también para la AEPD

Para la Agencia este reto ha implicado abordar una profunda reorganización de su estructura interna, así como un impulso complementario para promover herramientas y orientaciones que faciliten la adaptación al Reglamento por parte de responsables y encargados del tratamiento, y, en particular, las pymes.

La supresión de la obligación de notificar ficheros al Registro General de Protección de Datos; la mayor flexibilidad en el régimen de transferencias internacionales de datos con la eliminación, con carácter general, del régimen de autorizaciones; la nueva regulación de los códigos de conducta y la articulación del registro de Delegados de protección de datos ha supuesto una transformación sustancial de la Subdirección General del Registro de Protección de Datos, que ha asumido nuevas funciones relacionadas con la atención de consultas de los ciudadanos y responsables y encargados del tratamiento, y la promoción de recursos y protocolos para facilitar el cumplimiento del RGPD. También ha asumido el impulso de acciones de difusión con los distintos sectores empresariales y profesionales y la suscripción de protocolos y convenios con las asociaciones representativas de los mismos. El detalle de estas iniciativas se recoge en otros apartados de esta memoria.

La obligación generalizada de notificación de violaciones de seguridad a la AEPD ha hecho necesario articular medidas internas de naturaleza preventiva que permitan el análisis y seguimiento de las brechas de seguridad notificadas, dirigidas a supervisar las medidas adoptadas para minimizar sus riesgos; reduciendo así a casos puntuales la exigencia de responsabilidades por infracción del Reglamento. Medidas que han implicado la atribución de esta función a la Unidad de Evaluación y Estudios Tecnológicos (UEET). La evolución de estas notificaciones, así como las actividades de la UEET en la elaboración de herramientas que faciliten el cumplimiento del Reglamento, la auditoría del modelo de certificación de Delegados de protección

de datos y el seguimiento de innovaciones tecnológicas se describen posteriormente.

Por otra parte, el Reglamento incorpora un nuevo modelo de supervisión que recoge de forma equilibrada un amplio abanico de medidas correctoras de posibles incumplimientos de la norma, tales como la advertencia, un apercibimiento aplicable con gran flexibilidad, ordenar una actuación específica en un plazo determinado o imponer una limitación temporal o definitiva del tratamiento de los datos.

Medidas correctoras que pueden permitir que se garantice el cumplimiento de la norma cuando se ha desarrollado una conducta diligente y proactiva documentada por parte de responsables o encargados del tratamiento y tiene lugar un incumplimiento por error o por una insuficiencia puntual en el tratamiento realizado.

El RGPD también contempla, por otro lado, un régimen de sanciones económicas que pueden llegar a alcanzar los diez millones de euros o hasta el 2% del volumen de negocio total anual global del ejercicio financiero anterior o, incluso, hasta los veinte millones de euros o el 4% del volumen de negocio antes citado.

Este modelo de supervisión se complementa con las indicaciones del considerando 131 del Reglamento cuando señala que “la autoridad de control que recibe una reclamación o detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas, debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes”.

Atendiendo a esta previsión el Real Decreto ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, previó la posibilidad de remitir las reclamaciones al Delegado de protección de datos para que responda en el

plazo de un mes, e igualmente la de remitirlas al responsable o encargado del tratamiento de aquellas organizaciones que no hubieran designado un Delegado de protección de datos, antes de resolver sobre su admisión a trámite, para que dé respuesta en el mismo plazo.

Previsión que se ha visto confirmada en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El Reglamento contempla, en caso de que exista una posible vulneración de sus previsiones, tres tipos de tratamientos a los que se aplican distintas normas procedimentales: los tratamientos transfronterizos definidos en su artículo 4.23; los transfronterizos con relevancia local en un Estado miembro al que se refiere su artículo 56, y, aquellos que tienen la condición de exclusivamente nacionales.

El Reglamento prevé una serie de trámites específicos para los dos primeros supuestos entre los que se encuentran los necesarios para determinar la competencia de la autoridad de control principal, así como los que permiten la adopción de una decisión consensuada entre las autoridades principal e interesadas en el procedimiento. Tanto el Real Decreto ley 5/2018, como, posteriormente la LOPDGDD, han incorporado las normas de procedimiento necesarias para la adaptación del derecho interno a las citadas previsiones del RGPD.

Las previsiones sobre la posible resolución extrajudicial de reclamaciones y las relacionadas con los tratamientos transfronterizos y los mecanismos de cooperación y coherencia, han determinado una relevante modificación organizativa en la estructura de la Subdirección General de Inspección de Datos cuya descripción y efectos sobre la tramitación de las reclamaciones se recogen en otros apartados de esta memoria.

Junto a las medidas de adaptación del derecho español al RGPD, la LOPDGDD introduce novedades y mejoras desarrollando algunos contenidos del mismo, refuerza los derechos de los ciudadanos, clarifica conceptos y dota de seguridad jurídica a los responsables del tratamiento.

Desde la perspectiva orgánica, la LOPDGDD ha modificado sustancialmente la estructura de la Dirección de la Agencia Española de Protección de Datos y el procedimiento de designación de sus miembros.

La Presidencia de la Agencia, que sigue siendo una autoridad administrativa independiente de ámbito estatal, está auxiliada por un Adjunto, en el que podrá delegar sus funciones excepto las relacionadas con los procedimientos en caso de posible vulneración de la normativa de protección de datos. A ambos les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado. Su designación exige una cualificación específica exigiendo que deben ser personas de reconocida competencia profesional en esta materia.

Asimismo, la LOPDGDD ha modificado parcialmente la composición del Consejo Consultivo de la Agencia, incorporando a un representante del Consejo General del Poder Judicial, como autoridad de control en relación con los tratamientos relativos a los ficheros jurisdiccionales, y ampliando la presencia de nuevos colectivos, como son, entre otros, los profesionales de la protección de datos y de la seguridad, organismos y entidades de supervisión y resolución extrajudicial de conflictos, las profesiones colegiadas y expertos propuestos por el Consejo de Consumidores y Usuarios y las organizaciones sindicales más representativas. También se incorpora un representante de la Administración General del Estado y un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.

1.2 Informes jurídicos

1.2.1 Consultas

Las consultas de mayor complejidad dirigidas a facilitar la normativa de protección de datos por parte del Gabinete Jurídico de la Agencia se han visto, asimismo, condicionadas por la adaptación al RGPD. Se atendieron un total de 194, de las cuales 138 (71%) fueron planteadas por las Administraciones Públicas y 56 (29%) por el sector privado.

En 2018 se registró una disminución de un 42% en el volumen de consultas de las AAPP y el sector privado respecto a 2017

Produciéndose una disminución significativa en las consultas formuladas tanto por el sector público como por el sector privado, que disminuyen un 33% y un 56%, respectivamente.

Ello se debe a que parte de las consultas que plantean una problemática más sencilla han sido atendidas por otras unidades de la Agencia, como la Subdirección General del Registro, reservándose el informe del Gabinete Jurídico a las que revisten mayor complejidad.

En cuanto a las materias objeto de consulta cabe destacar que la aplicación del Reglamento General de Protección de datos y la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ha dado lugar a que se planteen cuestiones nuevas en directa relación con la interpretación de dichas normas.

Debe así hacerse referencia, especialmente, a los informes en que se pone de manifiesto la opinión de la Agencia en materias en que la

nueva regulación ha promovido un gran debate social.

En este sentido, cabe destacar, en primer lugar, el informe emitido como consecuencia de la alarma social despertada por la regulación del tratamiento de datos relativos a opiniones políticas por los partidos políticos al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, modificado por la disposición final tercera de la Ley Orgánica 3/2018,.

Dicho informe, tras determinar que tales tratamientos están sujetos a lo establecido en el Reglamento General de Protección de datos y a la Ley 3/2018, subraya que deben ser objeto de una interpretación restrictiva. Analiza a continuación detenidamente la base jurídica del tratamiento; los sujetos legitimados para realizar el mismo; su finalidad, que debe quedar circunscrita a la propaganda y actos de campaña electoral y, por tanto, dentro de la finalidad genérica de captación de sufragios a que se refiere la LOREG; los datos personales que pueden ser objeto de tratamiento, que estarán limitados a las “opiniones políticas de las personas obtenidas de páginas web y otras fuentes de acceso público”; la proporcionalidad del tratamiento limitando la elaboración de perfiles a perfiles generales de modo que los partidos políticos puedan conocer las inquietudes políticas de la ciudadanía, incluso por categorías genéricas como la edad, sexo, población, etc., sin que pueda, en ningún caso, pretenderse la realización de perfiles individuales o realizados atendiendo a categorías muy específicas que conculcarían los derechos fundamentales reconocidos en la Constitución Española. Y, por último, detalla las garantías que los responsables del tratamiento deben establecer, en particular las relativas al establecimiento de garantías técnicas apropiadas como la seudonimización e incluso la agregación o anonimización y la

realización de la correspondiente evaluación de impacto y, en su caso, la preceptiva consulta ante esta Agencia si la evaluación muestra que el tratamiento entraña un alto riesgo y el responsable no puede garantizar la adopción de medidas adecuadas para mitigarlo. Y se añade que, en el caso de que puedan adoptarse medidas que mitiguen el riesgo, deberán remitir a la Agencia el análisis realizado, la evaluación de impacto y la justificación de las medidas adoptadas.

En segundo lugar, los informes han dado respuesta a la inquietud mostrada en el ámbito científico de que la plena aplicación del RGPD supusiera un obstáculo para la investigación biomédica. Esta incertidumbre dio lugar también a la emisión de un informe en el que se analiza la incidencia que en el ámbito de la investigación biomédica pueda producir la aplicación de dicha norma. Tras analizar las normas del RGPD que resultan de aplicación, concluye que el régimen contenido en la normativa reguladora de la investigación biomédica no solamente se mantiene inalterado, sino que cabe una interpretación más flexible respecto al alcance que pueda darse a las finalidades del consentimiento prestado, superando incluso la interpretación más restrictiva contenida en el artículo 60 de la Ley de Investigación biomédica. Dicho informe apunta, asimismo, a que los comités éticos de investigación puedan tener en cuenta la interpretación no restrictiva efectuada en el informe respecto de las finalidades de investigación, en los supuestos en que autorizen el tratamiento de muestras codificadas sin contar con el consentimiento, conforme al artículo 58.2 de la Ley 14/2007, de Investigación biomédica.

En otro orden de cosas, cabe mencionar los informes emitidos en relación con las nuevas obligaciones impuestas por el RGPD, en particular, en relación con el nombramiento del delegado de protección de datos.

Se examina así en diversos informes la posibilidad de que el cargo de delegado de protección de datos del RGPD y el de responsable de seguridad del Esquema Nacional de Seguridad recaigan en la misma persona. Tales informes, partiendo del análisis de las funciones de cada una de estas figuras según su normativa específica, vienen a concluir que, con carácter general, debe existir la necesaria separación entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del citado Esquema Nacional de Seguridad, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

Por otra parte, han continuado efectuándose consultas en aquellas materias que tradicionalmente daban lugar a la emisión de mayor número de informes, en particular, la legitimación para el tratamiento de datos personales, referidas ahora a la interpretación que debe darse a los preceptos en esta materia del Reglamento General de Protección de Datos.

En este sentido, los informes emitidos vienen a reiterar el criterio de esta Agencia de que el RGPD pone en pie de igualdad las causas legitimadoras establecidas en su artículo 6, frente a lo dispuesto en la Ley Orgánica 15/1999 para la que el consentimiento venía a ser el eje central del derecho a la protección de datos.

Se examina así qué causas legitimadoras distintas al consentimiento resultan aplicables a los diversos tratamientos. A este respecto se considera que la prevista en el artículo 6.1.b del RGPD, esto es, el tratamiento necesario para la ejecución de un contrato en el que el interesado es parte, puede amparar para el tratamiento de datos de la relación empleado-empleador, la suscripción de seguros colectivos contratados en cumplimiento de la normativa laboral y o convenios colectivos, o las transmisiones de datos que sean precisas para llevar a cabo la gestión de las nóminas o las que se efectúen a corredurías o entidades aseguradoras con las que se contraten seguros colectivos, al ser necesarias estas transmisiones para el

adecuado y normal desenvolvimiento del contrato. Dicha base legitimadora amparará también el tratamiento de datos de familiares o personas relacionadas con los trabajadores como beneficiarios de seguros colectivos o planes de pensiones.

El cumplimiento de una obligación legal aplicable al responsable del tratamiento, conforme a lo previsto en el artículo 6.1.c) del RGPD vendrá a amparar el tratamiento de los datos relativos al porcentaje de discapacidad para la correcta realización de la correspondiente retención tributaria y el tratamiento de los datos necesarios para la deducción y abono a los sindicatos de la cuota de afiliación sindical.

No obstante, en el ámbito de vigilancia de la salud, será necesario con carácter general el consentimiento del empleado, según se desprende de lo previsto en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

En este mismo sentido, se ha efectuado un análisis de las bases jurídicas que legitiman el tratamiento de datos por la Administración Pública. Se aclara así que el sentido de la expresión “obligación legal” contenida en el artículo 6.1.c) RGPD equivale, en la regulación española de protección de datos, a “obligación establecida en una norma con rango de ley”, siendo éste un criterio asentado en la LOPDGD.

En cuanto a la extensión de la expresión contenida en la letra e) del artículo 6.1, esto es, “tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable” y si todo tratamiento de datos personales efectuado por la Administración Pública estaría en todo caso amparado por lo dispuesto en dicha letra e), se señala que los tratamientos de datos están sujetos a los principios del RGPD, entre ellos el de minimización, por lo que sólo estarán amparados en tal precepto los tratamientos de datos

personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron tratados. Asimismo, se recuerda que la Administración ha de actuar siempre vinculada a la ley y al Derecho, de modo que solo puede llevar a cabo aquello que el ordenamiento jurídico le permite expresamente (doctrina de la vinculación positiva de la Administración) y, en consecuencia, para que la Administración pueda actuar necesita de una previa habilitación legal y ello tanto si actúa en el ámbito del derecho público como en el ámbito del derecho privado.

En todo caso, el RGPD excluye la posibilidad de que los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones puedan tener como base jurídica la letra f) del artículo 6.1 RGPD, esto es el interés legítimo prevalente sobre los derechos y libertades de los interesados, debiendo interpretarse que el apartado e) del artículo 6.1 RGPD debe entenderse en sentido amplio de forma que permita a las Administraciones, incluso en el ámbito del derecho privado, los tratamientos de datos personales necesarios para las finalidades legítimas que el ordenamiento les permite.

Otro aspecto que se debe subrayar es el relativo a las cesiones masivas de datos entre Administraciones Públicas. Debe tenerse en cuenta que el deber de colaboración entre Administraciones Públicas está sujeto a lo previsto en el artículo 155 de la propia ley 40/2015, que limita el acceso a los datos que cada Administración debe facilitar a las restantes a lo previsto en la normativa de protección de datos de carácter personal, de modo que no cabe un acceso masivo e indiscriminado a datos personales. Debe aquí recordarse lo señalado en la Sentencia 19/2013 del Tribunal Constitucional debiendo ser tal acceso específico en cada caso y ajustado a los datos que resulten precisos para la tramitación de un expediente determinado.

Respecto a la cesión de datos entre Administraciones en los casos en que la finalidad del tratamiento para el que se solicita la cesión sea diferente a la inicial para la que se recabaron esos datos, habrá que ver en primer lugar, si existe una norma del derecho de la Unión Europea o del Estado miembro que permita el tratamiento para salvaguardar los objetivos del artículo 23.1 RGPD, siendo en tal caso el tratamiento “lícito” por disposición del propio RGPD. Si no existiese dicha norma, el responsable deberá determinar si la finalidad distinta de la inicial para la que se recogieron los datos es compatible con aquella, tras realizar un análisis de las circunstancias conforme a los criterios previstos en el artículo 6.4 RGPD. Se trata, en definitiva, de intentar evitar que existan lo que ha dado en denominarse “ciudadanos de cristal”, de modo que cualquier Administración no ha de tener un conocimiento expandido de todos los aspectos posibles de la personalidad de los ciudadanos, incluso de aquellos aspectos que sean innecesarios o superfluos para el ejercicio de sus potestades, conferidas por el ordenamiento para el interés público. Pero del mismo modo no cabe considerar que la normativa de protección de datos pueda resultar en una limitación irrazonable al ejercicio de dichos poderes públicos.

En lo que respecta a la legitimación para el tratamiento cuando el responsable no sea una Administración Pública cabe hacer referencia a los informes en los que se examina si el interés legítimo del responsable puede operar como base legitimadora.

Así, en lo que respecta al envío de comunicaciones comerciales por medios electrónicos se mantiene el reiterado criterio de la Agencia de que resulta de aplicación el principio de especialidad, de forma que las causas legitimadoras para el tratamiento de los datos a las que se refiere el artículo 6 del Reglamento General de Protección de Datos ceden ante la regla especial contenida, para estos concretos tratamientos, en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de

la información y de comercio electrónico, que viene a exigir el previo consentimiento del destinatario de las mismas, salvo cuando exista una relación contractual previa y el envío de comunicaciones comerciales se refiera a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En el supuesto de las comunicaciones comerciales por medios no electrónicos, podría resultar de aplicación lo previsto en la letra f) del artículo 6.1, del RGPD, según el cual podrá tener lugar el tratamiento, en el ámbito del sector privado, si el mismo “es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.” Para efectuar dicha ponderación, se tiene en cuenta que si la anteriormente citada Ley 34/2002, que mantiene un régimen especialmente estricto a la hora de obtener el consentimiento del interesado, efectúa la excepción a que antes se ha hecho referencia, tal regla sería aplicable por analogía a los supuestos en que los requisitos son menos rigurosos como en el caso de las acciones realizadas a través de otros canales de comunicación.

Para ello se requiere, de una parte, una interpretación razonable de lo que debe ser considerado como un producto o servicio similar al previamente contratado y, de otra, que tal ponderación se aplique solamente a los supuestos en que el interesado no haya cesado en su relación con la entidad. Por otro lado, para la licitud de estos tratamientos deben cumplirse el resto de requisitos establecidos en la normativa de protección de datos, en particular, los relativos al cumplimiento del deber de información previsto en los artículos 13 y 14 del RGPD, la garantía del derecho de oposición previsto en los apartados 2 y 3 del artículo 21 RGPD y la aplicación de la regulación de los

sistemas de exclusión publicitaria contenida en el artículo 23 de la Ley Orgánica 3/2018. Por último, debe recordarse que no prevalecerá el interés legítimo del consultante cuando la mercadotecnia o el envío de comunicaciones parta de la elaboración de perfiles exhaustivos del interesado mediante la combinación de diferentes fuentes de información para las que no ha dado su consentimiento.

Igualmente, en esta materia se ha valorado si la publicación de los datos de productividad de los empleados en una empresa podía fundamentarse en lo previsto en el artículo 6.1.f) del RGPD. Se entendió así que existía un interés legítimo en dicha publicación dado que su finalidad era generar una competitividad sana entre los empleados que ayude a mejorar la productividad general, así como a un interés legítimo de los propios empleados que, de este modo, podían conocer su propio rendimiento en comparación con el resto de compañeros de la empresa y se garantizaba además la transparencia de este dato que tiene su correspondiente repercusión económica. Para determinar la prevalencia de tal interés legítimo sobre los derechos de los particulares se tuvo en cuenta que se procedía a identificar a cada trabajador por su número de matrícula, dato que solo conoce el propio empleado y las personas del Departamento de Recursos Humanos, debiendo adoptarse las medidas organizativas y técnicas necesarias para evitar el acceso al resto de datos personales y la identificación individual de cada trabajador por personas no autorizadas, debiendo quedar suficientemente garantizado el secreto de dichos datos.

Asimismo, se entendía que la publicación se realizaba de una manera que resultaba menos perjudicial para el interesado, en tanto que sólo tenían acceso los propios empleados, evitando su difusión a personas que no forman parte de la relación laboral.

Informes preceptivos

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 2018 fueron informadas 64 disposiciones de carácter general, lo que supone una disminución del 35% respecto al ejercicio anterior. Ello se debe, en gran parte, a que, con la plena aplicabilidad del Reglamento (UE) 2016/679, a partir de 25 de mayo de 2018 desaparece la obligación de notificar e inscribir los ficheros en el Registro General de Protección de Datos y, en consecuencia, dejan de publicarse las correspondientes disposiciones de creación de éstos por parte de los distintos departamentos ministeriales y otras entidades que eran objeto de informe por esta Agencia.

Entre las disposiciones informadas en el año 2018 cabe mencionar las siguientes:

Anteproyecto de Ley Orgánica sobre la utilización de los datos de registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y otros delitos graves.

Anteproyecto de Ley por la que se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Anteproyecto de Ley de Servicios de Pago.

Anteproyecto de Ley para la transformación digital del sistema financiero.

Anteproyecto de Ley por la que se modifica texto refundido de la Ley de Regulación de los planes y fondos de pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre, para la transposición de la Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2016, relativa a las actividades y supervisión de los fondos de pensiones de empleo.

Anteproyecto de Ley por el que se modifica el texto refundido de la Ley de tráfico, circulación de vehículos a motor y seguridad vial, aprobado por Real Decreto Ley 6/2015, de 30 de octubre, en materia de permiso y licencia de conducción por puntos.

Proyecto de Real Decreto por el que se aprueba el Reglamento de ejecución de la Ley 45/2015 de 14 de octubre de voluntariado.

Proyecto de Real Decreto por el que se modifica el Real Decreto 954/2015 de 23 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros.

Proyecto de Real Decreto sobre justificación y optimización del uso de las radiaciones ionizantes para la protección radiológica de las personas con ocasión de exposiciones médicas.

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 las condiciones de utilización de la lengua de signos española y los medios de apoyo a la comunicación oral para las personas sordas, con discapacidad auditiva y sordociegas.

Proyecto de Real Decreto por el que se aprueba el reglamento general de la gestión financiera de la seguridad social.

Proyecto de Real Decreto por el que se desarrollan la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en materia de actuación y funcionamiento del sector público por medios electrónicos.

Proyecto de Real Decreto por el que se regula la reutilización de la información del Sector Público Estatal.

Proyecto de Real Decreto por el que se establecen las obligaciones de registro e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor.

Proyecto de Real Decreto por el que se regulan los estudios observacionales con medicamentos.

Proyecto de Real Decreto de desarrollo de normas legales que adaptan el derecho español a la normativa Europea en materia del mercado de valores.

Proyecto de Real Decreto sobre la determinación de la aptitud psicofísica del personal de la Guardia Civil.

Proyecto de Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 3/2013, de 20 de junio, en materia de lucha contra el dopaje en la actividad deportiva.

Proyecto de Real Decreto por el que se modifica el Real Decreto 180/2015 que regula el traslado de residuos en el interior del territorio de Estado.

Proyecto de Real Decreto por el que se modifica el RD.1345/2007, de 11 de octubre, por el que se regula el procedimiento de autorización, registro y condiciones de dispensación de los medicamentos de uso humano fabricados industrialmente.

Proyecto de Real Decreto por el que se regula el Registro General de establecimientos en el sector de la alimentación animal, y se establecen las condiciones de autorización de los puntos de entrada nacionales.

Proyecto de Orden por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Educación, Cultura y Deporte.

Proyecto de Orden por la que se establece el modelo y las normas reguladoras del expediente académico del personal de la Guardia Civil.

Proyecto de Orden sobre los datos a remitir al Registro Público Concursal regulado en el artículo 198 de la Ley 22/2018 de 9 de julio, concursal, a efectos de publicidad.

Proyecto de Orden ministerial por la que se ordena el Boletín Oficial del Ministerio de Defensa.

Proyecto de Orden por la que se constituye y regula el Registro unificado sobre Certificados y Centros de Formación de gases fluorados.

Proyecto de Orden por la que se modifica la orden SPI/2136/2011, 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 Decreto por el que se regula la actuación de la Administración de la Comunidad Autónoma de Extremadura en materia de adopción.

Proyecto de Decreto por el que se crea el Registro de Pacientes con Enfermedades Raras de la Comunidad Autónoma de Galicia. Separado por autoridad de protección de datos.

Proyecto de Decreto por el que se determina la asunción de las funciones en materia de protección de datos del Consejo de Transparencia y Protección de Datos de Andalucía.

Anteproyecto de Orden por la que se crea la Sede Judicial Electrónica de la Comunidad Autónoma de La Rioja.

Proyecto de Orden de la Conselleria de Justicia, Administración Pública, Reformas Democráticas y Libertades Políticas por la que se crea la Sede Judicial Electrónica de la Comunitat Valenciana.

Asimismo, se informó el anteproyecto de Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales. Norma cuyo objeto es la transposición de la Directiva (UE) 2016/680, que debió tener lugar para su aplicación efectiva el 25 de mayo de 2018.

1.3 Sentencias

El análisis del grado de seguridad jurídica en la aplicación de la normativa de protección de datos obliga a contemplar en qué medida las resoluciones de la AEPD son ratificadas o revocadas por los Tribunales.

Durante el año 2018 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional 164 sentencias, referidas todas ellas a la Ley Orgánica 15/1999, de 13 de diciembre, de las cuales:

- ▲ 94 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (57%).
- ▲ 11 estimaron parcialmente los recursos (7%).
- ▲ 45 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (27%).
- ▲ 14 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (9%).

El número de sentencias dictadas durante el año 2018 es similar al año anterior, si bien se ha producido un importante cambio en los sectores de actividad a que afectan las sentencias dictadas.

Ha descendido la litigiosidad en los sectores de banca, seguros y energía, que representan un 18% frente al 55% del año anterior y, especialmente, en el de las telecomunicaciones, que se reduce a un 10% del total, mientras que en el año anterior suponían un 27%

Resulta especialmente significativo el incremento de recursos formulados por particulares que pasan de suponer un 23% a un 40% del total. No obstante, un alto número de ellas son desestimadas, bien por la falta de legitimación activa del denunciante cuando únicamente se pretende la imposición de una sanción en un procedimiento, bien porque no se han aportado datos suficientes para abrir una actuación investigadora, o bien porque las cuestiones denunciadas eran ajenas al ámbito competencial de la AEPD.

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

En cuanto al ámbito de aplicación de la Ley Orgánica 15/1999, las sentencias de 29 de noviembre y 21 de diciembre declaran que no constituye un ámbito doméstico el tratamiento de datos efectuado por una empresa que presta un servicio consistente en que, a través de una aplicación de la que es titular, permite a un usuario tercero enviar bromas consistentes en un archivo de audio pregrabado vía telefónica al número de destino seleccionado por dicho usuario. Confirma la Audiencia el criterio de esta Agencia al considerar que dicha empresa, que alega ser un mero facilitador de una actividad que realiza el usuario en el ámbito

estrictamente personal o doméstico, efectúa un tratamiento de datos al registrar los números de teléfono de los denunciantes para realizar la llamada en cuestión y su voz, que se graba y esos datos personales de los denunciantes receptores de las bromas son incorporados a un fichero titularidad de dicha empresa, por lo que no puede considerarse su actividad limitada a un ámbito personal o doméstico.

En lo que respecta a la aplicabilidad de la LOPD, ambas sentencias ponen de manifiesto que el dato relativo a la voz de las personas grabadas constituye un dato de carácter personal.

La Sentencia de 21 de diciembre de 2018 sobre el concepto de dato personal en los formularios de unas encuestas considera que existe una codificación que permite a quien las efectuaba asociar los datos recogidos en el formulario de la encuesta a un domicilio concreto, por lo que se puede llevar a cabo la identificación sin grandes esfuerzos y no es posible apreciar la disociación de los datos. Se pronuncia asimismo sobre el carácter de dato especialmente protegido de los datos recabados, considerando que una de las finalidades expresamente reconocidas del tratamiento en cuestión es la de proporcionar una consulta de naturaleza ideológica y estimular la participación en la misma. Dicha finalidad está relacionada con el contenido de las encuestas realizadas, ya que indudablemente plantea unas preguntas relacionadas con la posición ideológica de los encuestados, concluyendo así que se efectúa un tratamiento de datos de ideología de las personas que cumplimentan dicha encuesta, ello tomando en consideración el contenido de las preguntas que, indudablemente, parten de una determinada posición ideológica que ha de ser aceptada para poder contestarlas. La encuesta se inclina claramente en favor de una determinada posición ideológica, con la que necesariamente ha de estarse conforme pues en otro caso no es posible contestar a la misma o al menos no en su integridad.

Se pronuncia asimismo sobre el concepto de fichero, considerando la existencia de éste. El encuestador introducía los datos personales de los encuestados y el resultado de la encuesta a la vez, por lo que existía correspondencia entre lo que había declarado la persona y sus datos de carácter personal. Se trata de criterios de archivo que posibilitan la localización de los datos personales, información que fue obtenida con la finalidad de ser conservada para permitir su utilización según se expone en el propio formulario encuesta. Se trata así de un fichero de datos personales en el sentido regulado en la LOPD, en la Directiva 95/46/CE y en el nuevo RGPD, pues la información que se recoge está constituida por datos personales y está también presente el elemento de organización que permite diferenciar este supuesto del referido a los libros de bautismo que venían a constituir una pura acumulación de datos.

De dicha sentencia cabe hacer referencia también a otros tres importantes aspectos, el relativo a la existencia de una conducta infractora, concretado en el presente caso en la recogida de datos personales relativos a ideología respecto de las personas que negaron su consentimiento para dicho tratamiento de datos, o respecto de personas que ni siquiera conocían que dicha recogida de datos personales se estaba produciendo. En segundo lugar, respecto a la responsabilidad solidaria por una única infracción alegada, se considera que debe declararse una responsabilidad individual de cada una de las personas jurídicas sancionadas, en tanto que el responsable del fichero o tratamiento puede venir constituido por una persona o por varias y en el presente caso ambas reconocen su responsabilidad plena y a título individual en el propio formulario de la encuesta. En tercer lugar, en lo que respecta a la proporcionalidad de la sanción y a la aplicación del artículo 45.5 LOPD, considera la sentencia adecuada la aplicación de una infracción grave, al tener en cuenta la actuación desarrollada por las entidades sancionadas en respuesta al requerimiento de la AEPD, consistente en la cesación en la utilización ilícita de datos de

personas que negaron su participación en la encuesta o no consintieron expresamente el tratamiento de sus datos fue atendido eliminando la información. Además, tras el requerimiento de la Agencia, también separaron la parte de la encuesta relativa a las respuestas de la referida a los datos personales del encuestado y su consentimiento.

En aspectos procedimentales resulta igualmente de gran interés la sentencia de 14 de diciembre de 2018, referida al ejercicio del derecho a la defensa y a la aplicación del principio non bis in idem. En lo que respecta a la primera de las cuestiones, se alegaba la vulneración del derecho a la defensa en el procedimiento sancionador que le impone la obligación de inmovilizar un determinado fichero ya que no se le hizo ningún requerimiento previo a la persona física recurrente sino a la empresa titular. Señala la sentencia que no cabe apreciar que se haya producido indefensión material al demandante, toda vez que como manifestaba la Sentencia del Tribunal Supremo de 8 de junio de 2015, que estimaba el recurso del representante legal de la Administración contra la sentencia de 15 de marzo de la AN, aunque ese requerimiento no se hizo personalmente a dicha persona no podía ser desconocido por éste, en cuanto administrador único de la empresa, encargado de los tratamientos del fichero y propietario del mismo.

Asimismo, se señalaba que ha conocido todas las actuaciones de la AEPD, sabía que el fichero estaba inmovilizado, no respetó la prohibición de utilizarlo e, incoado ese procedimiento, se le notificó tal hecho, participó activamente en el expediente, impugnó en él cuanto consideró conveniente a su derecho, se le notificó la propuesta de resolución, alegó contra ella y recurrió en reposición la resolución sancionadora, no advirtiéndose en tal secuencia ningún rasgo de indefensión.

En lo que se refiere a la aplicación del principio non bis in idem, señala la AN que hay doble sanción en el caso de que se haya sancionado

dos veces por los mismos hechos, pero en el caso de autos, no se ha sancionado más que una vez, pues el procedimiento sancionador anterior, que se siguió en su día, no terminó en sanción alguna, por la obvia razón de que el procedimiento terminó en caducidad. Y recuerda que la declaración de caducidad del procedimiento no implica la prescripción ni impide el ulterior ejercicio del ius puniendi en un nuevo procedimiento, como de manera reiterada ha declarado el Tribunal Supremo.

Debe también hacerse referencia a los siguientes aspectos analizados en las sentencias de la Audiencia Nacional:

En lo que respecta al ámbito de aplicación territorial de la LOPD, la Sentencia de 7 de octubre considera que el mero hecho de que una empresa sea titular de una cuenta corriente y un apartado de correos en España no son indicios suficientes de la existencia de establecimiento a los efectos de la aplicación de la LOPD. Sin embargo, dicho criterio ha sido corregido por la Sentencia del Tribunal Supremo de 5 de febrero de 2019, que entiende que el artículo 2.1.a) LOPD debe interpretarse de forma flexible y antiformalista, en el sentido de que resultan comprendidos el tratamiento de datos personales que se realiza en el marco o en el contexto de la actuación desarrollada en un Estado miembro de la Unión Europea (distinto a donde tiene la sede o administración principal) a través de la utilización de medios instrumentales que se revelen idóneos y eficaces en el tratamiento de datos personales.

También respecto al ámbito de aplicación territorial la Sentencia de 26 de enero de 2018, declara que la mera adquisición de una cantidad mínima de participaciones sociales en una empresa española, no se puede considerar como vínculo de conexión suficiente con la Unión Europea para aplicar ni la legislación europea ni la española a una reclamación efectuada por una persona de nacionalidad paraguaya y no residente en ningún estado de la Unión Europea, en relación a determinadas

noticias aparecidas en diarios de su país que afectan a su persona y son accesibles a través del buscador Google.

En relación con la legitimación para el tratamiento, la sentencia de 2 de enero considera legítima la actuación de un Servicio público de salud de una comunidad autónoma que remitió información sobre la historia clínica de una persona al juzgado de lo social, atendiendo al requerimiento efectuado por el órgano judicial, a pesar de tratarse de información médica cancelada y bloqueada, ya que tal comunicación resulta una excepción a dicha obligación de bloqueo, expresamente contemplada en la normativa de aplicación.

La sentencia de 27 de febrero confirma la falta de legitimación para el envío de mensajes por SMS recordando el cargo de recibos, ya que el interesado se había opuesto a su recepción. Señala la sentencia que el envío de tales mensajes no era preciso para el desarrollo de la relación contractual, que podía llevarse a cabo sin necesidad de dicho tratamiento por lo que el artículo 6.2 de la LOPD no sirve de cobertura para tal tratamiento.

La sentencia sobre legitimación para consultar los ficheros de solvencia refleja que no cabe un acceso indiscriminado a tales ficheros sino que podrán ser consultados por un tercero cuando precise enjuiciar la solvencia del afectado

Considera la sentencia que el artículo 42 del RLOPD que establece los supuestos en que se permite el acceso, tiene un carácter de *numerus apertus*, por lo que no resulta necesaria una relación contractual o precontractual para que

una entidad crediticia o de riesgo pueda hacer uso de la facultad prevista en dicho artículo siempre que exista un interés legítimo para tal acceso.

En lo que respecta al ejercicio de derechos, la sentencia de 12 de junio, relativa a la cancelación en la historia clínica de anotaciones relativas al procedimiento de reasignación de género, incluido el nombre de género ya en desuso, considera que no procede aquélla por no haber transcurrido el plazo mínimo de conservación de los datos exigido por la ley de autonomía del paciente, pero sí debe efectuarse la cancelación respecto de las menciones de género que figuren como inexactas en los informes que consten en la historia clínica. También en relación con la historia clínica, la sentencia de 9 de febrero señala que no quedan comprendidos en el derecho de acceso, los accesos realizados por terceros a la historia clínica.

En relación con la cancelación de antecedentes policiales las sentencias de 23 de julio y 5 de octubre exigen una adecuada justificación por parte de la autoridad administrativa de las razones por las que se restringe o deniega el derecho de cancelación, sin que baste el mero silencio administrativo ni la utilización de fórmulas genéricas o estereotipadas que no permitan apreciar las razones en las que se sustenta la limitación del derecho. La sentencia de 8 de noviembre concluye que, ante la insuficiencia de motivación, se ha vulnerado el derecho de cancelación del demandante en relación con los datos personales que de él obran en el fichero de gestión de antecedentes de las personas de interés policial, por lo que procede reconocer su derecho a la cancelación pretendida, en relación con los datos consistentes en los antecedentes policiales solicitados.

En sentencia de 30 de enero se confirma que no procede la cancelación de los datos de número de teléfono y dirección de correo electrónico de un empleado de un Ayuntamiento, adscrito al servicio de extinción de incendios, resultando

una medida idónea y necesaria para asegurar la correcta prestación del servicio y la protección de intereses tales como la vida y la integridad de las personas y sus bienes o la protección del medio ambiente, y proporcionada porque el titular de los datos solicita la cancelación de todos ellos, sin ofrecer otros que garanticen la posibilidad de contactar con él.

En cuanto a las sentencias relacionadas con el derecho de los afectados a la supresión de enlaces en motores de búsqueda, son numerosas las sentencias en las que se da prevalencia al derecho a la libertad de expresión sobre el derecho a la protección de datos respecto a las opiniones y juicios vertidos por el afectado en el ámbito profesional.

En sentencia de 27 de abril se considera prevalente el derecho a la libertad de información porque no constan las referencias que se hacen en las URLs al denunciante, elemento indispensable para determinar si debe prevalecer el interés público o el derecho a la protección de datos del interesado. En Sentencia de 12 de junio, se hace referencia a la prevalencia del derecho a la información sobre el derecho a la protección de datos, en la información publicada en un periódico relativa a una sentencia en la que se relataba la participación en un delito de abuso sexual por el que fue condenado el denunciante. En sentencia de 27 de noviembre considera que prevalece el interés público en el acceso a la publicación de las listas de candidatos a las elecciones generales y autonómicas, publicidad que tiene carácter obligatorio y en el caso denunciado el transcurso del tiempo no puede considerarse excesivo. De la misma manera en Sentencia de 11 de diciembre se considera que prevalece el derecho a la libertad de expresión sin que pueda considerarse que la información publicada sea obsoleta. Sin embargo, en sentencia de 5 de enero considera prevalente el derecho a la protección de datos de la recurrente, al tratarse de datos excesivos ya que se difunden datos personales de su esposo, ascendientes, religión, etc., que nada tienen que ver con el ejercicio de

su trabajo público y nada aportan a una crítica de su actividad profesional.

Sobre los ficheros de solvencia, la sentencia de 6 de febrero confirma que para que los datos existentes en el fichero de solvencia cumplieran con la exigencia del artículo 4.3 de la LOPD, relativo al principio de veracidad o exactitud, debería reflejarse la existencia de las diferentes entidades informantes y las respectivas fechas en las cuales comunicaron los datos al fichero.

Como en el año anterior, varias sentencias se refieren al incumplimiento del requisito del requerimiento de pago, se sigue en esta materia por la AN el criterio de que no puede imputarse la falta de requerimiento a quien adquirió una deuda que ya estaba incluida en el fichero de solvencia, habiéndose producido el requerimiento por la cedente y notificado la inclusión. En sentencia de 19 de enero, se entiende que no existe requerimiento previo, ya que lo único que consta en las actuaciones al respecto, es una carta dirigida a un domicilio que no era en ese momento el del denunciante, cuando el real le constaba en la base de datos a la entidad recurrente, y así se lo comunicó a los ficheros de solvencia patrimonial.

La sentencia de 28 de febrero considera válida la notificación intentada en un apartado postal, que figuraba también como dirección del denunciante ante el fichero ASNEF y a la que notificó su inclusión en dicho fichero y otras comunicaciones que fueron recibidas sin problema y fue la dirección facilitada en la denuncia a la AEPD y donde recibió las notificaciones de esta.

La sentencia de 8 de junio entiende que ha sido la conducta del deudor la que provocó que el requerimiento de pago, efectuado mediante carta certificada, no fuera retirado dejándolo caducar y que el requirente ha cumplido con la diligencia exigible a fin de cumplir con su obligación de requerimiento previo a la inclusión de la deuda en el fichero de morosidad. La sentencia de 14 de diciembre considera que

el cesionario de unos datos realizó los trámites necesarios para realizar el requerimiento previo a la inclusión de los datos de la denunciante, remitiendo dicho requerimiento al domicilio que le fue cedido cuando adquirió la cartera de créditos, desconociendo que se trataba de una deuda derivada de una contratación fraudulenta. Entiende la Audiencia que nos encontramos ante un tercero que actuó de buena fe y sin conocimiento del origen de la deuda, únicamente de la deuda en sí.

En la sentencia de 2 de marzo, en relación con un requerimiento previo de pago por e-mail, se declara que el envío efectivo de un correo electrónico por parte del servidor del correo de origen no implica su recepción por el servidor del correo del destinatario, siendo ello así porque la confirmación de la recepción de los correos electrónicos depende del funcionamiento del resto de los servidores de correo electrónico intervinientes en la comunicación y especialmente de los servidores de las cuentas de correo destinatarias y el gerente del proveedor de servicios informáticos no aporta elementos que respalden que el correo electrónico fue recepcionado en destino.

Igualmente, se han dictado diversas sentencias relacionadas con el tratamiento ilícito de datos en supuestos de contratación irregular. En Sentencia de 3 de mayo se señala que el denunciante utiliza, según el caso, hasta 4 ó 5 firmas distintas, concluyendo que no es posible deducir de tal divergencia entre sus firmas la falta de consentimiento.

En sentencia de 19 de octubre se considera se ha actuado con la diligencia adecuada en la formalización de la relación contractual, observando las normas que regulan el consentimiento verbal en las solicitudes de portabilidad de líneas, en tanto que el contenido de la grabación se ajusta plenamente a las condiciones estipuladas por la circular 1/2009 de la CMT y añade que tan pronto la entidad tuvo conocimiento de que se había producido una posible suplantación de personalidad en

la contratación de la línea móvil en cuestión, procedió a la anulación de las facturas emitidas y a excluir los datos de los ficheros de solvencia patrimonial y crédito.

En el ámbito del marketing, se considera vulnerada la LOPD en el caso de realización de llamadas a quien se había opuesto a las mismas ante un operador telefónico, porque el prestador de un servicio de telemarketing subcontratado sin su consentimiento utilizó para llamar al denunciante datos procedentes de sus propios ficheros, sin que conste que, con carácter previo, hubiera cruzado tales datos procedentes de sus propios sistemas de información con el fichero Robinson del operador. No obstante, el operador resulta responsable a título de culpa, al haberse desentendido y no haber supervisado el uso de los datos efectuado por su encargado de tratamiento, y ello con independencia de la responsabilidad en que hubiera podido incurrir tal encargado del tratamiento, al actuar por su cuenta y riesgo y al margen de las instrucciones establecidas por el operador en el contrato.

Por su parte, el Tribunal Supremo dictó un total de 4 resoluciones (3 sentencias y 1 auto) referidas a recursos de casación interpuestos frente a sentencias dictadas en procesos en los que era parte la Agencia. En relación con estos recursos: declaró en tres 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 otro supuesto la inadmisión del recurso. En consecuencia, el Tribunal Supremo confirmó en los 4 asuntos que llegaron a su conocimiento el criterio que había mantenido la Agencia Española de Protección de Datos.

También el Tribunal Constitucional se ha pronunciado en una Sentencia sobre el derecho al olvido, considerando que el ejercicio del derecho así denominado respecto de datos veraces que figuran en una hemeroteca digital prohibiendo indexar los nombres y apellidos para su uso por el motor de búsqueda interno debe ser considerada una medida limitativa de

la libertad de información idónea necesaria y proporcionada al fin de evitar una difusión de la noticia lesiva de los derechos invocados.

En relación con la jurisprudencia del Tribunal de Justicia de la Unión Europea recaída en materia de protección de datos durante el año 2018 resulta relevante reseñar tres sentencias. Las dos primeras son particularmente importantes por cuanto que en ellas se describen supuestos en los que el Tribunal concluye que es aplicable la figura del corresponsable del tratamiento. Esta figura, definida específicamente en el RGPD, está siendo objeto de debate en el Comité Europeo de Protección de Datos (CEPD) y, previsiblemente, dará lugar a nuevas y novedosas fórmulas de responsabilidad en la aplicación del RGPD.

La primera de ellas, de 5 de junio de 2018, asunto C-210/16, es la planteada por el Bundesverwaltungsgericht (Tribunal Supremo de lo Contencioso-Administrativo, Alemania) en el contexto de un litigio entre el Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Autoridad regional independiente de protección de datos de Schleswig-Holstein, Alemania, "UDL") y Wirtschaftsakademie Schleswig-Holstein GmbH, sociedad de Derecho privado especializada en el ámbito de la educación, respecto a la legalidad de una orden emitida por la UDD para que esta última desactivara su página de fans alojada en el sitio de la red social Facebook.

Declara aquí el Tribunal que el artículo 2.d) de la Directiva 95/46/CE debe interpretarse en el sentido de que el concepto de «responsable del tratamiento», comprende al administrador de una página de fans alojada en una red social. Declara también que los artículos 4 y 28 de la Directiva 95/46 deben interpretarse en el sentido de que, cuando una empresa establecida fuera de la Unión dispone de varios establecimientos en diversos Estados miembros, la autoridad de control de un Estado miembro está facultada para ejercer los poderes que le confiere el artículo 28, apartado 3, de la mencionada

Directiva respecto a un establecimiento de esa empresa situado en el territorio de ese Estado miembro, aun cuando, en virtud del reparto de funciones dentro del grupo, por un lado, este establecimiento únicamente se encarga de la venta de espacios publicitarios y de otras actividades de marketing en el territorio de dicho Estado miembro y, por otro lado, la responsabilidad exclusiva de la recogida y del tratamiento de los datos personales incumbe, para todo el territorio de la Unión, a un establecimiento situado en otro Estado miembro.

Asimismo, el Tribunal concluye que el responsable de la red social y el administrador de la página de fans alojada en ella, son conjuntamente responsables del tratamiento. Si bien, aclarando que dicha responsabilidad conjunta no se traduce necesariamente en una responsabilidad equivalente, ya que ésta debe graduarse en atención a las distintas etapas del tratamiento.

Por último determina que el artículo 4.1.a) y el artículo 28 números 3 y 6 de la citada directiva deben interpretarse en el sentido de que, cuando la autoridad de control de un Estado miembro pretende ejercer frente a una entidad establecida en el territorio de ese Estado miembro los poderes de intervención contemplados en el artículo 28, apartado 3 de la referida Directiva, debido a infracciones de las normas relativas a la protección de datos personales cometidas por un tercero responsable del tratamiento de esos datos que tiene su domicilio en otro Estado miembro, dicha autoridad de control es competente para apreciar, de manera autónoma respecto de la autoridad de control de este último Estado miembro, la legalidad del referido tratamiento de datos y puede ejercer sus poderes de intervención frente a la entidad establecida en su territorio sin instar previamente la intervención de la autoridad de control del otro Estado miembro.

La segunda de las sentencias, de 10 de julio

de 2018, asunto C-25/17, fue planteada el Korkein hallinto-oikeus (Tribunal Supremo de lo Contencioso-Administrativo, Finlandia) en el marco de un procedimiento incoado a instancias del tietosuojavaltuutettu (Supervisor de protección de datos, Finlandia), relativo a la legalidad de una resolución de la tietosuojalautakunta (Comisión de protección de datos, Finlandia) que prohíbe a la Jehovan todistajat — uskonnollinen yhdyskunta (comunidad religiosa de los Testigos de Jehová; en lo sucesivo, «comunidad de los Testigos de Jehová») recoger o tratar datos personales en relación con la actividad de predicación puerta a puerta sin que concurran los requisitos de la legislación finlandesa relativa al tratamiento de datos personales.

El Tribunal declara al respecto, en primer lugar, que la recogida de datos personales llevada a cabo por miembros de una comunidad religiosa en relación con una actividad de predicación puerta a puerta y el tratamiento posterior de esos datos no constituyen ni tratamientos de datos personales efectuados en el ejercicio de actividades contempladas en el artículo 3.2 de dicha Directiva, esto es, actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, ni tratamientos de datos personales efectuados por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

En segundo lugar, manifiesta que el concepto de «fichero», definido en el artículo 2.c de la citada directiva, comprende un conjunto de datos personales recogidos en relación con una actividad de predicación puerta a puerta, consistentes en nombres, direcciones y otra información relativa a las personas contactadas, siempre que los datos estén estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. Para que dicho conjunto de datos esté comprendido en ese concepto no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda.

En último lugar, declara que el 2.d) de la

Directiva 95/46, en relación con el artículo 10.1 de Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que permite considerar que una comunidad religiosa es responsable, junto con sus miembros predicadores, de los tratamientos de datos personales efectuados por estos últimos en relación con una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad, sin que sea necesario que la comunidad tenga acceso a los datos ni haga falta demostrar que ha impartido a sus miembros instrucciones por escrito o consignas en relación con esos tratamiento.

La última de las sentencias a reseñar es la de 2 de octubre de 2018, asunto C-207/16, Ministerio Fiscal. Se trata de una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona y tiene por objeto, la interpretación del artículo 15.1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, en relación a la denegación de acceso de la Policía Judicial a datos personales almacenados por proveedores de servicios de comunicaciones electrónicas.

El Tribunal declara que dicho precepto debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

1.4 El Comité Europeo de Protección de Datos

La aplicación efectiva del Reglamento General de Protección de Datos (RGPD), así como la simultánea finalización del plazo para la transposición de la Directiva sobre protección de datos en los ámbitos policial y judicial penal ha supuesto uno de los principales retos al que se han enfrentado las autoridades de supervisión.

En el plano europeo, tanto el anterior Grupo Europeo de Autoridades de Protección de Datos (Grupo del Artículo 29) como su sucesor, el Comité Europeo de Protección de Datos (CEPD), han sido plenamente conscientes de la necesidad de ofrecer guías para la aplicación coherente y armonizada de esas normas, sin perjuicio de seguir dedicando atención a algunas de las principales cuestiones planteadas en materia de protección de datos.

En ese sentido, una de las primeras decisiones del Comité Europeo de Protección de Datos en el día mismo de su constitución fue la de ratificar las directrices que el Grupo del Artículo 29 había ido preparando con vistas a la entrada en aplicación del RGPD.

En concreto, el Comité refrendó los siguientes documentos:

- ▲ Directrices sobre identificación de la autoridad principal según el RGPD
- ▲ Directrices sobre aplicación y determinación de multas administrativas en el marco del RGPD
- ▲ Directrices sobre Delegados de Protección de Datos
- ▲ Directrices sobre Portabilidad en el RGPD
- ▲ Directrices sobre Decisiones individuales automatizadas y Perfilado en el RGPD
- ▲ Directrices sobre Consentimiento según el RGPD

- ▲ Directrices sobre Transparencia según el RGPD
- ▲ Directrices sobre Notificación de Violaciones de Seguridad según el RGPD
- ▲ Marco de Adecuación en el RGPD
- ▲ Directrices sobre varios aspectos relativos a las BCR en el RGPD

Posteriormente, el Comité, ya constituido como tal, siguió en la misma línea y adoptó los siguientes documentos:

- ▲ Directrices sobre las excepciones previstas en el artículo 49 RGPD (transferencias internacionales)
- ▲ Directrices sobre certificación e identificación de criterios de certificación según los artículos 42 y 43 RGPD
- ▲ Directrices sobre acreditación de entidades de certificación según el artículo 43 RGPD
- ▲ Dictamen relativo a la Propuesta de Decisión de Aplicación de la Comisión Europea sobre la protección de datos adecuada en Japón
- ▲ Directrices sobre el ámbito territorial del RGPD (Artículo 3)

Como se ha señalado, la mayor parte de estos documentos persiguen aclarar la interpretación y alcance de algunas de las principales disposiciones del RGPD. Varios de ellos, en concreto los que fueron adoptados por el Grupo del Artículo 29 en los años 2016 y 2017, han sido ya tratados en anteriores Memorias de la Agencia. Varios de los aprobados por el Comité en 2018 tienen una especial relevancia, por motivos diversos.

Es el caso de las Directrices sobre las excepciones previstas por el artículo 49 del RGPD en el ámbito de las transferencias internacionales. El RGPD diseña un sistema de transferencias internacionales que, en

congruencia con el principio de accountability que informa todo su contenido, limita al mínimo indispensable los casos en que las transferencias a países terceros u organizaciones internacionales requieren de autorización por parte de las autoridades de supervisión.

Ello implica que es importante que, por parte de las autoridades, en este caso del Comité Europeo, se establezcan criterios y directrices precisos sobre el modo en que deben aplicarse las previsiones del Reglamento y la utilización de los diversos instrumentos que contempla.

En ese sentido, estas Directrices acompañan a otros documentos ya citados, como son los relativos al Marco de Adecuación en el RGPD o a los diversos textos que han buscado actualizar la posición del Comité en materia de Normas Corporativas Vinculantes (BCR, por sus siglas en inglés).

El documento sobre excepciones es también una actualización de otros anteriores adoptados por el Grupo del Artículo 29. En él se pasa revista a las excepciones que, según el artículo 49 RGPD, permiten la transferencia internacional de datos personales en ausencia de una decisión de adecuación o de garantías suficientes.

El documento subraya el carácter “excepcional” que debe tener la aplicación de los diversos supuestos que contempla el artículo 49 y también la estrecha vinculación que debe existir respecto a la necesidad de la transferencia. En ese sentido, se considera que transferencias regulares o sistemáticas no debieran ampararse en estas excepciones.

De hecho, el documento señala que, aunque el propio RGPD admite que la excepción del “interés público”, puede ser, justamente, una excepción a esa regla y servir para fundamentar transferencias que se realicen de una forma más continuada y no esporádica, el Comité aconseja que cuando sea éste el caso, los organismos públicos afectados (u otros privados que sirvan también fines de interés público) busquen

alternativas más estructuradas y que ofrezcan unas mayores garantías a los afectados.

Dado su objetivo de actualización, las Directrices se centran en las excepciones que presentan algún tipo de novedad frente a la Directiva 95/46/CE, como sucede con la del consentimiento, que en este caso ha de ser explícito, o con la que permite las transferencias sobre la base de un “interés legítimo imperioso” del responsable. En este punto, el Comité confirma la interpretación que se había hecho por parte de la AEPD en el sentido de que la información que el responsable ha de proporcionar a la autoridad de supervisión ha de remitirse con anterioridad a que la transferencia se produzca.

Las Directrices sobre certificación e identificación de criterios de acreditación, junto con las Directrices sobre acreditación de organismos de certificación, reflejan también el interés del Comité en abordar desde los primeros momentos de aplicación del RGPD los nuevos mecanismos de autorregulación que el Reglamento establece en el marco de las medidas de cumplimiento.

Mientras que los códigos de conducta ya estaban incluidos, aunque con mucho menor detalle y extensión, en la Directiva 95/46, los esquemas de certificación, sellos y marcas se presentan como una nueva opción a disposición de las organizaciones que, de una manera proactiva, deseen demostrar su alineamiento con las previsiones del Reglamento. Sin embargo, las disposiciones del Reglamento, si bien son bastante más detalladas que las originariamente incluidas por la Comisión en la propuesta original, siguen careciendo de precisión y claridad en algunos aspectos fundamentales.

Las Directrices sobre certificación analizan cuestiones tales como la definición de los principales conceptos utilizados por el RGPD, el papel de las autoridades de supervisión y de las entidades de certificación, y la aprobación y desarrollo de los criterios de certificación.

El segundo de estos documentos, por su parte, analiza el concepto de acreditación en el marco del RGPD, los papeles respectivos de las autoridades de supervisión, actuando o no como organismos de acreditación, el papel de las autoridades nacionales de acreditación, y los criterios de acreditación propiamente dichos. Debe señalarse que el Comité está elaborando también su posición en relación con el otro instrumento de autorregulación citado, los códigos de conducta. Más en concreto, se está desarrollando un documento sobre códigos de conducta y organismos de supervisión, cuya aprobación estaba prevista para febrero de 2019. Un elemento importante de estas directrices es que las autoridades de supervisión nacionales tendrán que tomarlas como referencia para elaborar sus criterios de acreditación de los organismos de supervisión de los códigos de conducta, que habrán de ser sometidos a la aprobación del Comité Europeo.

Las Directrices sobre aplicación del artículo 3 del RGPD tratan también de otra de las principales novedades del Reglamento. Como es sabido, este artículo mantiene el criterio tradicional de aplicación basado en el establecimiento de responsables o encargados en el territorio de la Unión, pero reemplaza el tradicional criterio del uso de medios por el más actualizado del objetivo o “targetting”.

El Reglamento prevé que será de aplicación a los tratamientos que realicen responsables o encargados no establecidos en la Unión cuando esos tratamientos estén relacionados con la oferta de bienes o servicios a personas en la Unión, esté o no asociada a una contraprestación económica, o con el control de su actividad.

La novedad de esta última previsión, y también algunos aspectos del criterio clásico de la presencia en territorio de la Unión, han impulsado al Comité a adoptar este documento, que a finales de 2018 había sido aprobado en su primera versión por el Comité y se encontraba en fase de consulta pública.

El documento analiza elementos como la noción de oferta “dirigida a personas en la Unión”, la noción de “control de la actividad” y también dedica atención especial al papel y responsabilidades del representante en la Unión que deben designar los responsables y encargados a los que resulta de aplicación el RGPD en virtud del artículo 3.2 del RGPD.

Un último documento que merece comentario en este apartado es el Dictamen sobre la propuesta de decisión de adecuación de Japón presentada por la Comisión. La Comisión adoptó su propuesta de decisión sobre la adecuación de Japón a comienzos de septiembre de 2018. A finales de ese mismo mes, solicitó el dictamen del CEPD, según lo previsto en el artículo 70.1.s. RGPD.

Esta solicitud de dictamen tuvo tres características singulares. Por un lado, se trataba de la primera vez en que el Comité emitiría un dictamen sobre una propuesta de decisión de adecuación en el marco del RGPD. Por otra parte, el régimen de protección de datos de Japón, a diferencia de lo que ha sucedido en la mayoría de los casos de adecuación, difiere en su estructura y enfoque del modelo europeo, aproximándose más el proceso de análisis al que se siguió por parte del antiguo Grupo del Artículo 29 con relación al Privacy Shield estadounidense. Finalmente, el interés político de la Comisión en conseguir publicar la decisión a la mayor brevedad hizo que el plazo que se concedió al Comité fuera muy corto, teniendo en cuenta la complejidad de la labor a desarrollar. Este último aspecto evidenciaba, en este campo concreto, lo que se ha puesto ya de manifiesto en otros ámbitos, que es lo reducido de los plazos que el Reglamento concede al Comité para adoptar dictámenes y decisiones.

El Comité adoptó su dictamen sobre la propuesta de decisión en diciembre de 2018. Hay que destacar, no obstante, que, durante los trabajos de preparación del dictamen, y como consecuencia de las observaciones y preguntas planteadas por el equipo de trabajo del Comité,

la Comisión modificó en dos ocasiones su propuesta. Estas modificaciones ilustran el nuevo grado de influencia que se atribuye a las posiciones del Comité.

En su dictamen, el Comité reconoce que hay importantes áreas de convergencia entre la legislación japonesa y la europea. También reconoce los esfuerzos realizados para aproximar la legislación japonesa a la europea en materia de protección de datos.

El Comité reconoce que existen grandes paralelismos entre la normativa japonesa y la normativa europea

La ley japonesa de protección de datos presenta una serie de vacíos normativos que hacen que, en sí misma, no resulte equiparable a la europea. Esos vacíos se han salvado mediante la adopción, por parte de la autoridad de supervisión japonesa, de unas normas adicionales, las “Supplementary Rules”, que serán aplicables específicamente a los datos que sean transferidos desde la Unión a Japón.

Este último punto, no obstante, junto con ser un elemento favorable en la valoración, plantea también algunas dudas al Comité. Las autoridades japonesas han insistido en que son normas que se cumplen por las empresas, que aplica la propia autoridad de supervisión y que son utilizadas por los tribunales. Pero no han llegado a afirmar que tengan un carácter formalmente vinculante. Por ello, el Comité invita a la Comisión a hacer un seguimiento estrecho de la aplicación y el cumplimiento de estas normas.

Aparte de esta cuestión, el Comité muestra también preocupación por todo lo relativo a las transferencias ulteriores de datos enviados a Japón, en particular, cuando

esas transferencias ulteriores se realicen a países considerados “adecuados” en virtud de la legislación japonesa. Las autoridades japonesas se han comprometido a aplicar una serie de salvaguardas para estas decisiones de adecuación, entre ellas la de informar a la Unión Europea.

Sin embargo, el Comité, insiste en la necesidad de que la Comisión tome las medidas necesarias para asegurar que se mantiene el nivel de protección o, alternativamente, decida la suspensión de la decisión.

Un área a la que se prestó especial atención, siguiendo la pauta ya establecida en relación con el Privacy Shield, y en aplicación de los criterios establecidos por la Sentencia del Tribunal de Justicia de la Unión en el Caso Schrems, es la del acceso de las autoridades públicas japonesas con finalidades de “law enforcement” o seguridad nacional a los datos transferidos desde la Unión. El Comité reconoce que existen grandes paralelismos entre la normativa japonesa y la normativa europea, así como que las autoridades japonesas han asegurado que no se accede a información en manos de empresas por motivos de seguridad nacional más que si éstas la proporcionan voluntariamente o cuando esta información se encuentra en fuentes accesibles al público. El Comité, no obstante, se hace eco también de la existencia de preocupaciones reflejadas en medios de comunicación y en informaciones de expertos sobre la realidad práctica de estas limitaciones.

Aun cuando se trata de dictámenes de diferente naturaleza, debe subrayarse que el Comité ha aprobado también durante 2018 los relativos a las listas de tratamientos que requieren de la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) presentadas por las autoridades nacionales.

La autorización del Comité, vía dictamen, está prevista tanto en el artículo 35.4 como en el 64.1 del RGPD. El objetivo de estas listas es

proporcionar a los ciudadanos y las empresas de la Unión Europea unas directrices claras sobre los tratamientos que las autoridades consideran que son susceptibles de comportar un alto riesgo para los derechos y libertades de las personas físicas.

Las listas presentadas por las autoridades, y los correspondientes dictámenes, están basadas en los criterios establecidos por el Grupo del Artículo 29 en sus “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD”.

El objetivo que se persigue con la autorización del Comité es conseguir la armonización de las listas para los tratamientos transfronterizos, aunque las listas pueden incluir tratamientos exclusivamente nacionales, que no serán objeto de valoración por parte del CEPD.

En el periodo de julio a diciembre de 2018 se presentó la práctica totalidad de listas nacionales, que fueron autorizadas por el Comité con, en general, pocas salvedades respecto a los textos propuestos originariamente. La AEPD presentará la suya en enero de 2019, estando previsto que sea aprobada en el mes de marzo de 2019.



1.5 Adecuación de la AEPD al RGPD

Además de las reestructuraciones organizativas que se describen en otros apartados, la adaptación de la AEPD al RGPD ha seguido un proceso estructurado en 15 tareas, que supusieron un total de 25 acciones diferentes llevadas a cabo desde octubre de 2017 a mayo 2018 y que han sido informadas por el Delegado de Protección de Datos (DPD) de la AEPD al Comité de Dirección.

Después de la asignación de recursos al proyecto y la designación, con fecha 31 de octubre de 2017, del DPD de la AEPD comenzaron las tareas de adecuación al RGPD, revisando la política de seguridad de la información de la AEPD para construir un documento único sobre la política de protección de datos y seguridad de la información y el documento de obligaciones del personal.

De forma paralela se comenzó la construcción del registro de actividades de tratamiento de la AEPD, en un proceso de desarrollo continuo a través de su categorización, realización del análisis de riesgo sobre los derechos y libertades de las personas y, como conclusión del mismo, la elaboración de las acciones correctivas de adecuación de los sistemas de información de la AEPD al RGPD.

Se decidió realizar una evaluación de impacto, de acuerdo a los criterios que el RGPD señala, sobre aquellas actividades que pudieran tratar categorías especiales de datos o de menores para aislar aquellos tratamientos, que, aunque perfeccionados durante la actividad de la AEPD en estos años, pudieran ser significativos en la repercusión que tienen sobre los derechos de las personas.

Se elaboraron las cláusulas informativas sobre las distintas actividades de tratamiento descritas en el registro de actividades con objeto de atender el derecho de información, elaborando también cláusulas informativas

para su inclusión en los contratos de encargado del tratamiento. Cada una de las acciones realizadas se llevó a cabo en consonancia y relación con las demás, convirtiendo el proceso de adaptación al RGPD en un proceso continuo de revisión y corrección.

En todo este proceso se ha trabajado en la documentación de los elementos que sirven para gestionar de forma proactiva el cumplimiento del RGPD, así como en el seguimiento de la implantación de las medidas correctivas señaladas en el plan de acción del análisis de riesgos y de la evaluación de impacto.

1.6 Tecnológicos

El Reglamento incluye entre las funciones propias de las autoridades de control, la de “hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular, el desarrollo de las tecnologías de la información y las prácticas comerciales” (art. 57.1.i).

Con el fin de incorporar a su organización una unidad específica que permitiera impulsar esta función de la Agencia, de forma complementaria pero independiente de las competentes para promover el modelo de cumplimiento y de supervisión del RGPD, se creó en el año 2015 la Unidad de Evaluación y Estudios Tecnológicos (UEET). Esta Unidad ha desarrollado diferentes actividades de cooperación con asociaciones y universidades. Asimismo, dicha unidad ha participado en la elaboración de guías para facilitar la implementación del Reglamento General de Protección de Datos, tales como la “Guía práctica para las evaluaciones de impacto en la protección de datos personales”, la “Guía de análisis de riesgos” y la “Guía para la gestión y notificación de brechas de seguridad”.

Por otra parte, la unidad ha supervisado el Esquema de Certificación para Delegados de Protección de Datos y ha asumido el análisis de las notificaciones de brechas de seguridad y de las consultas sobre evaluaciones de impacto.

Su actividad durante el año 2018 se describe a continuación:

▲ 1.6.1 Investigación sobre proyectos tecnológicos

La AEPD ha prestado atención a la adecuación de los tratamientos que se basan en las tecnologías disruptivas más allá de las actuaciones derivadas de la potestad sancionadora, y está desarrollando un importante trabajo para identificar los riesgos de dichos tratamientos con el objeto de gestionarlos mediante las garantías adecuadas.

La Agencia se ha posicionado en la investigación de los retos tecnológicos y, entre otras actuaciones, participa en proyectos desarrollados en el marco de las subvenciones de la Comisión denominadas Horizonte 2020, como, el proyecto SMOOTH para el desarrollo de herramientas de ayuda al cumplimiento del RGPD de las pymes y micropymes europeas, en donde se está llevando a cabo el seguimiento y asesoramiento en los tratamientos de datos previstos durante el desarrollo de estas herramientas.

También ha participado en la financiación e inicio del proyecto PANELFIT para uso ético de las TIC y en la propuesta del proyecto APPRENTICE para la formación de excelencia de expertos en protección de datos dentro del campo de la ingeniería en el conjunto de acciones Marie Skłodowska Curie – H2020 y en la propuesta del proyecto IANUS para el uso de tecnologías disruptivas en el contexto de las actuaciones de las fuerzas y cuerpos de seguridad para la prevención del terrorismo.

1.6.2 Elaboración de guías

Con relación a la aplicación por los responsables y encargados de los principios de responsabilidad proactiva, la UEET ha colaborado en la elaboración de las Guías de Evaluaciones de Impacto para la Protección de Datos y de Análisis de Riesgos para los tratamientos de datos de carácter personal.

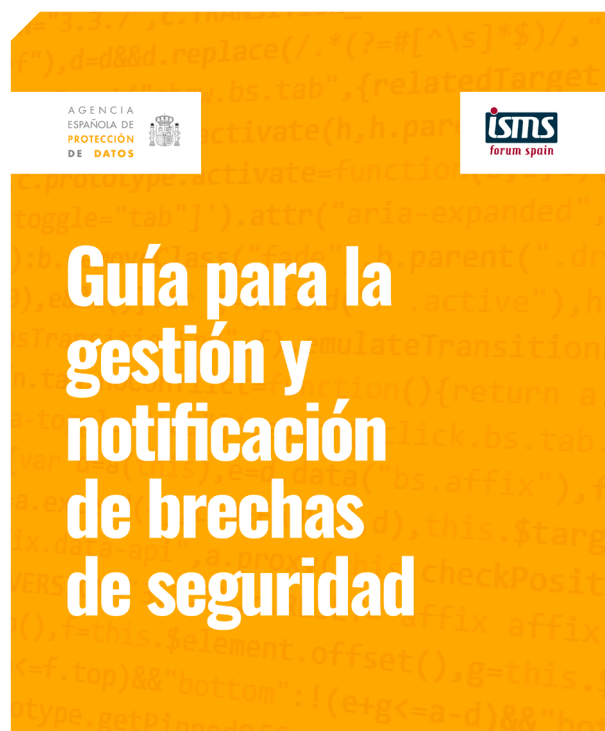
También, ha desarrollado una Guía para la gestión y notificación de brechas de seguridad, para implementar de forma efectiva el requisito que marca el RGPD para una protección eficaz de los intereses de los sujetos de los datos en caso de violaciones de seguridad.

1.6.3 Notificaciones de violaciones de seguridad (brechas de seguridad)

Junto a ello, la UEET ha intervenido en el análisis de las brechas de seguridad notificadas a la Agencia, así como en el de las consultas previas sobre evaluaciones de impacto.

A partir del 25 de mayo de 2018, es exigible en efecto la obligación de notificación de brechas de seguridad que afecten a datos de carácter personal, tanto a la autoridad de control como a los sujetos de los datos, a menos que sea improbable que constituya un riesgo para los derechos y libertades de las personas, por lo que la AEPD ha elaborado y puesto en marcha procedimientos para la gestión de las notificaciones de brechas de seguridad.

En la sede electrónica de la AEPD está disponible un formulario para la notificación de brechas de seguridad, siguiendo las recomendaciones establecidas por el Comité Europeo de Protección de Datos. También se ha desarrollado un trabajo para coordinar el portal de notificación de la AEPD con los portales de notificación de incidentes de seguridad del CCN y del INCIBE, una tarea que se prolongará a 2019.



En el marco señalado en los párrafos anteriores, desde el 25 mayo de 2018 hasta el 31 de diciembre han sido recibidas en esta Agencia un total de 547 notificaciones de las que, tras su análisis y clasificación, han sido remitidas a la Subdirección General de Inspección de Datos un total de 16 que afectaban a datos, principalmente, de salud, menores, ideología política y tratamientos masivos de datos.

1.6.4 Evaluaciones de impacto y consultas previas

El RGPD ha introducido otro aspecto también novedoso, como ha sido la obligación de la realización de las consultas previas sobre Evaluaciones de Impacto para aquellos tratamientos considerados de alto riesgo.

Además, el Reglamento establece la necesidad de realizar una consulta previa a la AEPD cuando el resultado de dicha evaluación evidencia que el riesgo que supone para los sujetos de los datos no ha podido ser mitigado por el conjunto de garantías definidas por el responsable.

Teniendo en cuenta la necesidad de evaluar las consultas previas remitidas por los responsables, la AEPD ha puesto en marcha procedimientos internos para la recepción y gestión de las mismas. Esto ha significado que durante 2018 se han recibido 44 solicitudes de consultas previas sobre evaluaciones de impacto. El análisis de las mismas ha mostrado que en 40 de ellas no se cumplían los requisitos que establece en el RGPD, respondiéndose a los remitentes en consecuencia, y dos de ellas fueron respondidas mediante el correspondiente informe, quedando las dos restantes en estudio a finales de año.

1.6.5 Certificación

Aunque fue en el año 2017 cuando se desarrolló en la AEPD, en colaboración con la Entidad Nacional de Acreditación (ENAC), el Esquema de Certificación para Delegados de Protección de Datos, en el marco de la norma ISO/IEC 17024:2012, y que en el mismo periodo se iniciaron las primeras actuaciones en el marco del Esquema, ha sido en 2018 cuando las entidades que se adhirieron al esquema y obtuvieron la acreditación profesional han iniciado sus actividades, lo que ha supuesto disponer de los primeros DPD certificados bajo el esquema de la Agencia.

Durante el año 2018, tres entidades certificadoras de DPD han obtenido la acreditación definitiva y ocho entidades han terminado el año con la designación provisional para la realización de actividades de certificación para obtener la acreditación definitiva

Para ello, la AEPD y ENAC han realizado auditorías conjuntas en dichas entidades, en un total de doce, y se ha desarrollado un banco de preguntas que permite generar los exámenes para la certificación de DPD que se encuentra en continua adaptación con el objetivo de homogeneizar el grado de complejidad de las pruebas para la certificación de DPD.

Esta certificación tiene validez en 70 países y ha tenido impacto internacional ya que se ha asesorado a otras autoridades de protección de datos como la Autoridad Coreana de Protección de Datos con relación al esquema de certificación para DPD y la Autoridad Francesa, CNIL.

1.6.6 Cooperación con asociaciones y otras entidades

En cuanto a las acciones de cooperación realizadas por la AEPD con otras entidades específicamente en el campo de tecnologías disruptivas o tratamientos que impliquen alto riesgo, se han realizado una veintena de acciones. A destacar, sin ser exhaustivo, la participación en el observatorio español de Big Data para el intercambio de experiencias en el uso de dicha tecnología y su desarrollo en la aplicación de técnicas de Inteligencia Artificial y de análisis de datos.

También se puede señalar como acción destacada por su impacto la colaboración con la iniciativa DPO Community impulsada por ISMS Forum Spain, con el objeto de impulsar la colaboración con los DPD del sector privado.

Sin señalar un foro concreto, pero subrayando una temática en la que se ha reclamado una mayor necesidad de colaboración, hay que destacar las colaboraciones sobre temas investigación científica, en particular en el marco de la salud. Este hecho pone de manifiesto la inquietud que en este campo ha despertado la aplicación del RGPD y la respuesta activa que ha mostrado la AEPD.

▲ 1.6.7 Colaboración con Universidades

En el marco del impulso a las tareas de formación en relación con el conocimiento del RGPD y de creación de una cultura de protección de datos común entre Europa y América, se celebró un convenio con la Universidad Nacional de Educación a Distancia para la creación de un Master de Protección de Datos para Iberoamérica.

La AEPD ha financiado un proyecto con la Universidad Politécnica de Madrid, a través de Fundetel para la realización del desarrollo de dos estudios sobre privacidad y protección de datos en los tratamientos personales en aplicaciones móviles. Este proyecto, bajo la supervisión de la AEPD, tiene como objeto último desarrollar la cultura de la Privacidad por Defecto y desde el Diseño en aplicaciones móviles, especialmente enfocados para emprendedores y nuevos desarrolladores.

En el marco del convenio con la Universidad Carlos III de Madrid, alumnos de postgrado han recibido formación en la AEPD, además de dirigir los trabajos de fin de master.



1.7 Plan estratégico

▲ 1.7.1 La ejecución del Plan Estratégico

Para el ejercicio 2018, tercer año de ejecución del plan estratégico, se habían previsto en la programación inicial del año un total de 74 iniciativas, pero a lo largo del ejercicio se han ido incorporando otras 7 actuaciones nuevas -no incluidas en el cronograma- y otra que sí estaba incluida pero que no se había contemplado en la programación inicial de 2018, en concreto la relativa a la actualización de la Guía de cookies.

Todo ello arroja una cifra total a final de año de 82 iniciativas para ejecutar a lo largo de 2018.

En razón a su periodo de ejecución, se distribuyen del siguiente modo:

▲ Iniciativas de ejecución continua o plurianual: 48

▲ Iniciativas de ejecución no continua o anual/bianual: 34

Las siete iniciativas incorporadas al cronograma del Plan para su ejecución durante 2018 han sido:

▲ Orientaciones/recomendaciones sobre juguetes conectados (9 bis)

▲ Actuaciones en el ámbito sanitario, farmacéutico y de la investigación biomédica (33 bis)

▲ Colaboración con la Comisión Nacional de los Mercados y la Competencia (43)

▲ Colaboración con el servicio 060 (Portal de Atención Ciudadana de la AGE) (44 bis)

▲ Encuentro sobre Compra Segura en Internet (88 bis)

▲ Listado de Cumplimiento Normativo (92 bis, 5)

- ▲ Encuentro con Delegados de Protección de Datos de las Diputaciones Provinciales (101 bis)

En cuanto a su grado de cumplimiento, hay que señalar que, respecto a las acciones continuas o plurianuales, todas ellas han podido llevar a cabo alguna actuación durante el ejercicio. Por lo que se refiere a las acciones no continuas o anuales, todas ellas igualmente han podido completarse, a excepción de la actualización de la Guía de cookies (51), la creación de un espacio Web para desarrolladores (68), y la elaboración de un tesoro de protección de datos para facilitar la búsqueda de la información disponible en la Web de la Agencia (84). Estas tres iniciativas, por distintas razones, no han podido ser ejecutadas durante el presente ejercicio, como se había programado inicialmente, y han pasado a formar parte de las actuaciones del Plan previstas para el próximo año 2019.

El conocimiento detallado de las actuaciones llevadas a cabo por la AEPD en relación con cada una de las 82 iniciativas se puede conocer en el “Informe 2018 de cumplimiento del Plan Estratégico de la AEPD”, accesible en la web de la Agencia.

Además de estas siete iniciativas incorporadas al cronograma del Plan para su ejecución en 2018, hay que reseñar que durante el ejercicio se han incorporado para su ejecución en 2019 otras 14 iniciativas más, que son las siguientes:

- ▲ Site Web sobre reclamaciones en materia de contratación eléctrica y gas (7 bis)
- ▲ Encuentro con Delegados de Protección de Datos de Universidades (27)
- ▲ Jornada sobre el RGPD con la Audiencia Nacional (41 bis)
- ▲ Orientaciones sobre el tratamiento de los datos personales en la actividad de los partidos políticos (48 bis)

- ▲ Convenio de colaboración con el Centro para el Desarrollo Tecnológico Industrial (CDTI) (62 bis)

- ▲ Estudio de privacidad en dispositivos y aplicaciones móviles para la monitorización de la actividad física, el bienestar y la salud (63 bis,1)

- ▲ Estudio de privacidad de aplicaciones para su uso en el aula en entornos de educación obligatoria (63 bis,2)

- ▲ Orientaciones en protección de datos para operadores de drones (64 bis)

- ▲ Análisis comparativo de privacidad en navegadores web (66 bis)

- ▲ Orientaciones sobre el tratamiento de datos biométricos (67 bis)

- ▲ Herramienta de evaluación de impacto en protección de datos (EIPD) para Administraciones Públicas (92 bis, 6)

- ▲ Herramienta de análisis de riesgos para PYME (92 bis, 7)

- ▲ Herramienta de evaluación de impacto en protección de datos (EIPD) para pymes (92 bis, 8)

- ▲ Estudio sobre los efectos de la adopción de la Directiva PNR (106 bis)

En consecuencia, a lo largo del ejercicio 2018 se han incorporado al Plan Estratégico, como iniciativas nuevas no programadas en el cronograma del mismo, un total de 21, siete de ellas para ejecutar en 2018, y las 14 restantes en 2019.

Todo lo cual hace necesario proceder a una actualización del cronograma general del Plan Estratégico, que inicialmente contemplaba un total de 113 iniciativas y que, tras las sucesivas revisiones, han pasado a ser 121 en 2016, 131 en 2017 y 148 a 3 de diciembre de 2018, tras la

incorporación de las mencionadas 21 iniciativas (7 a ejecutar en 2018 y 14 en 2019), y una vez descontadas las cuatro bajas. Es decir, a lo largo de estos tres años de vigencia del plan se ha producido un incremento en el número total de iniciativas a ejecutar de un 12%.

▲ 1.7.2 Marco de actuación de Responsabilidad Social (RS)

La protección de datos vive un momento determinante debido a los continuos cambios tecnológicos que impactan directamente en el ciudadano y, en especial, en colectivos vulnerables -como los menores y las mujeres- que nos conciencian, entre otras cosas, de que es necesario luchar contra la violencia en internet.

Para afrontar estos retos, durante este año la Agencia ha dado los primeros pasos para sentar las bases de un proyecto de Responsabilidad Social (RS) que supone la culminación de una etapa que se inició a finales de 2015 con la aprobación del Plan Estratégico de la AEPD 2015-2019.

Esta iniciativa refuerza aún más el compromiso de la Agencia con la privacidad y la protección de sus datos personales. Este compromiso, viniendo de un organismo regulador y del ámbito público, adquiere una especial responsabilidad, en lo que supone orientar su actividad hacia fines distintos a los meramente correctores y sancionadores. Pero, al mismo tiempo, es lo que da sentido a la actividad de un organismo público cuya razón de ser es la defensa y garantía de un derecho fundamental. Para hacerlo efectivo, no existe mejor marco que la Agenda 2030 y los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas. Y, para ello, lo primero que se ha hecho desde la Agencia ha sido contar con la colaboración del Pacto Mundial de Naciones Unidas, que ha llevado colaborado en la alineación del Plan Estratégico con la Agenda 2030. En concreto, se ha evaluado el impacto social de las 148 iniciativas del Plan Estratégico y cómo se relacionan con 10 de

los 17 ODS y las 169 metas de la Agenda 2030, constatándose que la Agencia impacta de manera especial en tres ODS:

- ▲ ODS 16: paz, justicia e instituciones sólidas
- ▲ ODS 12: producción y consumo responsables
- ▲ ODS 17: alianzas para lograr los objetivos



Como ejemplo, la AEPD puede influir en el ODS 16 y sus metas 16.5, 16.6, 16.7 y 16.10 que tratan temas tan relevantes como:

- ▲ Reducir considerablemente la corrupción y el soborno en todas sus formas
- ▲ Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas
- ▲ Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y acuerdos internacionales

En cuanto al ODS 12, la Agencia influye en las metas 12.6 y 12.8 que cubren temas como:

Asegurar que las personas de todo el mundo tengan la información y los conocimientos pertinentes para el desarrollo sostenible.

Hecha esta evaluación previa, el siguiente paso ha sido proceder a la elaboración de un Marco de Actuación de la AEPD en materia de RS para los próximos cinco años, que se aprobará durante 2019, una vez que sea sometido a la participación, a través de la web de la Agencia, de los empleados, las organizaciones y los ciudadanos en general, para que puedan remitir sus comentarios, sugerencias y aportaciones.

2. Al servicio de los ciudadanos

2.1 Consultas y FAQs

La AEPD ofrece a los ciudadanos, a través del Área de Atención al Ciudadano, varios canales mediante los cuales pueden plantear sus dudas respecto a la normativa de protección de datos: atención telefónica, presencial y por escrito, así como la posibilidad de realizar consultas a través de la Sede Electrónica, y de acceder al catálogo de las consultas más frecuentes (FAQs) que se encuentran publicadas en la citada Sede. El número total de consultas planteadas y respondidas por este Área durante el año 2018 ascendió a 749.020, lo que supone un incremento del 192,69% respecto al año 2017, en el que se atendieron 255.298 consultas. Este significativo incremento se debe a un importante aumento en el número de accesos a las preguntas frecuentes, que alcanzaron los 651.650, frente a los 170.754 del año 2017.

El desglose es el siguiente:

Atención presencial	3.455
Atención telefónica	88.302
Consultas por escrito	453
Consultas por la Sede electrónica	5160
Acceso a las preguntas frecuentes	651.650

El detalle de la evolución trianual puede consultarse en la sección de consultas recogida en el Anexo “La Agencia en cifras”.

Por otro lado, se ha producido un descenso en el número de consultas atendidas por escrito (5.613 frente a las 7.954 de 2017), que responde a la puesta en marcha del canal INFORMA_RGPD, creado en el mes de marzo para la atención a las consultas planteadas por los responsables y encargados del tratamiento, por sus organizaciones y asociaciones representativas y por sus delegados de protección de datos.

Los temas más consultados fueron los siguientes: el RGPD, cómo formular reclamaciones ante la AEPD, el funcionamiento de la herramienta FACILITA y el tratamiento de datos personales en los ficheros de solvencia patrimonial.

Con respecto a las consultas sobre el ejercicio de derechos por parte de los ciudadanos, cabe destacar que más del 62% se refirieron a los derechos con arreglo al RGPD (que ha introducido nuevos derechos, como el de limitación del tratamiento o el de portabilidad), un 14,8% versaron sobre el derecho de cancelación de la Ley 15/1999 y el 13,43% sobre el derecho de acceso. A estos derechos les siguieron el denominado derecho al olvido, con un 4%, y los de oposición y rectificación con un 2,89% y un 0,91%, respectivamente. Un 1,77% de estas consultas se refirieron a los requisitos para el ejercicio de estos derechos.

El catálogo de Preguntas Frecuentes (FAQs) ha sido renovado este año con motivo de la aplicación efectiva del Reglamento General de Protección de Datos a partir del 25 de mayo de 2018. En este sentido, se han reagrupado las preguntas correspondientes a las cuestiones generales del RGPD; la adecuación al RGPD; las transferencias internacionales, BCR y códigos de

conducta; y delegados de protección de datos y Certificación de delegados de protección de datos.

Además, se actualizaron a finales de año a efectos de contemplar las novedades introducidas por la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. Este catálogo permite consultar más de 200 preguntas-respuestas agrupadas por temas y, en muchas ocasiones, la oportuna respuesta se completa con el acceso a materiales publicados por la AEPD. Esta modificación ha supuesto, como ya se ha referido, que en el año 2018 haya tenido lugar un gran incremento del número de visitas, casi cuadruplicando la cifra correspondiente a 2017. Destaca el interés suscitado por la figura del delegado de protección de datos y su certificación, siendo estas preguntas las más consultadas, junto a las correspondientes a comunidades de propietarios y a videovigilancia.

2.2 Protección de los menores

Con la aprobación de la LOPDGDD se alcanzó uno de los objetivos que la Agencia perseguía desde hacía tiempo, como ha sido la inclusión del ámbito de la privacidad y el derecho a la protección de datos en el mundo online entre los contenidos de desarrollo curricular escolar, al establecerse en el artículo 83 el derecho a la educación digital, que ha de ser cumplido en el plazo de un año a contar desde el 7 de diciembre de 2018.

De este modo, la Ley incorpora una solución estructural que la Agencia había venido promoviendo con insistencia, como es la incorporación del conocimiento sobre la protección de datos personales en los currículos escolares y en los planes de formación del profesorado. Solución que sensibilizó tanto el Gobierno como de los grupos parlamentarios al incluir en la LOPDGDD el derecho a la educación digital, exigiendo a las Administraciones educativas su inclusión y desarrollo entre el

bloque de asignaturas de libre configuración para alcanzar la competencia digital del alumnado y garantizar su plena inserción en la sociedad digital y, dando el plazo antes señalado desde su entrada en vigor, para el cumplimiento de este mandato. La Agencia ha puesto de manifiesto su disposición a colaborar en el desarrollo de los materiales educativos necesarios para la aplicación efectiva de la Ley.

2.2.1 Canal Joven

La protección de los menores constituye uno de los ejes de actuación de la actividad de la Agencia Española de Protección de Datos, como se recoge en su Plan Estratégico y se constata a través de las actividades que en este ámbito se vienen desarrollando y que se reflejan en las memorias anteriores.

El enfoque se ha orientado en la prevención, para sensibilizar a los menores de la utilización responsable y segura de sus datos personales en internet y en particular en las redes sociales, así como en la concienciación tanto de las familias como de los profesores, pues son los actores clave de su formación y desarrollo como personas.



Respondiendo a este objetivo, la Agencia creó un canal específico para proporcionar la máxima información posible a todos los agentes intervinientes o interesados en el tratamiento de datos personales de los menores, el Canal Joven, que dispone de varias vías de comunicación dirigidas a dar respuesta a las cuestiones o dudas que se planteen referentes a este ámbito.

El Canal Joven integra, además de la dirección de correo electrónico canaljoven@agpd.es, un teléfono específico para consultas sobre temas de menores (901 233 144) y un servicio de información de WhatsApp (616 172 204). A las consultas que llegan por estos medios, se suman las recibidas a través de la Sede Electrónica de la Agencia que se derivan a equipo del Canal Joven.

A través de estas vías, se ha dado respuesta, durante 2018, a 1.564 consultas realizadas, lo que supone un incremento de casi el 74,75% con respecto a las 895 recibidas en 2017. Siendo las consultas más frecuentes las que se refieren a la toma de imágenes, quién lo puede hacer (profesores, familiares...) y si hace falta consentimiento para ello, tanto en las aulas como en eventos escolares y extraescolares (campamentos, excursiones, funciones teatrales...), así como quién debe otorgar el consentimiento para tratar datos personales de menores cuando los padres están separados.

▲ 2.2.2 Acciones de difusión, concienciación y fomento del derecho a la protección de datos

En esa labor de fomento de la información y promoción de la concienciación de los menores de edad sobre el buen uso de los datos personales en internet, el 10 de mayo se presentó el Manual “Protección de datos y prevención de delitos” elaborado en colaboración con la Fiscalía de Criminalidad Informática.

El manual tiene como finalidad dar a conocer conductas en el ámbito de internet que constituyen delitos y que en muchas ocasiones se cometen por menores sin saber que son comportamientos que tienen un reproche penal con arreglo a legislación sobre responsabilidad penal del menor, y consecuencias civiles de las que, en su caso, responden los padres.

El manual pone el foco en aquellas conductas que desde la perspectiva de la utilización de información personal en internet tienen relevancia en los tipos del código penal, además de constituir una infracción a la normativa de protección de datos, en la medida en que van desde utilizar y difundir, a través de la Red, datos de carácter personal de otras personas sin su consentimiento, o para fines distintos de los que estaban autorizados o consentidos, a conseguir de manera ilícita los datos de otras personas. El manual también recoge una serie de recomendaciones o consejos para evitar ser víctima de alguno de estos comportamientos. El manual se inserta en el marco de las actividades previstas en el Plan Estratégico 2015-2019 de la Agencia.

En este ámbito de la prevención y sensibilización se han llevado a otras acciones como la adaptación en formato televisivo para su difusión por este medio de la serie de vídeos “Tú controlas en internet” en los que se abordan situaciones como el ciberacoso, el grooming, el sexting, o la dependencia tecnológica y la huella digital, y que han sido objeto de difusión por diversas cadenas televisivas.

La Agencia ha participado en el MOOC para el Centro Regional de Formación del Profesorado de la Comunidad de Madrid “Seguridad, privacidad e identidad digital en el entorno escolar”, que pretende extenderse a otras Comunidades Autónomas, y en jornadas para la formación de inspectores de educación, a la vez que se mantiene la colaboración con los DPD de las Consejerías de Educación.

En el ámbito de la comunidad educativa se ha mantenido una reunión informativa con el vicepresidente de la Confederación Española de Asociaciones de Padres y Madres de Alumnos (CEAPA) sobre tratamientos de datos llevados a cabo por las AMPAS.

Durante la semana de la Administración Abierta se organizó en colaboración con el INJUVE una jornada de puertas abiertas sobre la privacidad y seguridad de los jóvenes en internet. Durante este taller se analizaron los riesgos en los que pueden incurrir los jóvenes por un uso inadecuado de la tecnología y las aplicaciones que ésta les proporciona, como las redes sociales. Además, se expusieron las herramientas que puede ofrecer la Agencia para salvaguardar y garantizar los derechos de los ciudadanos y especialmente los más jóvenes. Se han adaptado al RGPD la “Guía sobre protección de datos dirigida a los centros educativos”, las FAQs y el resto de los contenidos del espacio de la web de la Agencia dedicado a “Educación y menores” (www.tudecideseninternet.es), que en 2018 ha recibido 169.689 visitas a los distintas páginas de la web Tú decides en internet, que corresponden a 121.998 visitantes distintos, lo que supone un incremento del 20,99% y 153,98%, respectivamente.

Aunque en otro apartado se abordan más detenidamente los premios sobre protección de datos que anualmente convoca la Agencia, en 2018 ha tenido lugar la segunda convocatoria del Premio a las “Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet”, que consta de dos categorías, una dirigida a los centros educativos y otra a las personas e instituciones que destaquen por el impulso de buenas prácticas en esta materia en relación con los menores, y que forma parte del conjunto de acciones que la Agencia desarrolla para reforzar la protección de los menores en el ámbito de la protección de datos.

2.3 Comunicación

Como en años anteriores, la Agencia ha desplegado a lo largo de 2018 múltiples acciones para dar visibilidad a las iniciativas realizadas. A continuación, se detallan las relacionadas con el departamento de prensa y comunicación, así como las acciones de divulgación realizadas en la página web de la Agencia, y su agenda institucional.

2.3.1 Redes sociales

El 28 de enero, coincidiendo con el Día Europeo de Protección de Datos, la AEPD lanzó su cuenta oficial de Twitter, cumpliendo así con su objetivo de estar presente en el entorno de las redes sociales, una de las medidas contempladas en el Plan Estratégico de la Agencia. Desde entonces, la cuenta de Twitter de la Agencia ha ido ganando seguidores a un ritmo de casi 260 a la semana hasta cerrar 2018 con más de 12.400 followers.

Con este nuevo canal, la Agencia persigue varios objetivos: dar a conocer la labor que desempeña la AEPD, promoviendo la sensibilización entre los ciudadanos en relación con la protección de sus datos, y difundir las guías, materiales y herramientas de cumplimiento que la Agencia pone a disposición de los profesionales, las empresas y las Administraciones Públicas.

Por otra parte, esta cuenta representa un instrumento esencial para conocer cuáles son las inquietudes en esta materia por parte de los diferentes colectivos, tanto de quienes tratan datos como de aquellas personas cuyos datos son objeto de tratamiento. Desde sus inicios, la cuenta de Twitter de la Agencia ha publicado numerosos tuits destinados a fomentar el conocimiento de los derechos y obligaciones del RGPD, tanto a ciudadanos como a organizaciones, mediante la difusión de materiales elaborados por la AEPD, como guías, herramientas para facilitar el cumplimiento, infografías o la retransmisión de eventos en los que participaban representantes de la Agencia.

Entre otros ejemplos, la cuenta de Twitter de la AEPD ha ayudado a difundir la Guía del ciudadano, y otras como las Guías de gestión y notificación de brechas de seguridad; de privacidad y seguridad en internet; de protección de datos y prevención de delitos; de compra segura en internet, así como las de análisis de riesgos y de evaluación de impacto en la protección de datos. Asimismo, ha dado difusión a diferentes secciones prácticas incluidas en la web.

Además, ha difundido infografías de elaboración propia, como las relacionadas con la adaptación al Reglamento por parte de las Administraciones Públicas y el sector privado; los derechos de los ciudadanos; los juguetes conectados, o el decálogo de protección de datos para el personal sanitario y administrativo. Adicionalmente, ha ofrecido información relacionada con foros en los que ha estado representada la Agencia o celebrados a iniciativa de esta, como la 10ª Sesión Anual Abierta de la AEPD.

A fecha 31 de diciembre de 2018, la cuenta de Twitter de la AEPD sumaba 1.300 tuits publicados, más de 700 consultas atendidas, cerca de 110.000 visitas al perfil de la Agencia, y más de siete millones de impresiones

▲ 2.3.2 El blog de la Agencia

El blog de la Agencia se ha consolidado como un canal adicional a través del cual la Agencia difunde el derecho fundamental a la protección de datos. Como ya hiciera en 2017, el blog dedicó gran parte de sus contenidos el año pasado a divulgar los nuevos derechos recogidos en

el Reglamento y cómo ejercerlos, así como a facilitar a los responsables del tratamiento de datos el cumplimiento de las obligaciones derivadas del mismo.

De los más de 88.000 accesos al blog que se registraron en 2017, se ha superado la cifra de 100.000 en 2018. ‘Qué es un DPD’, ‘De la inscripción de ficheros al registro de actividades’, ‘Cómo puedo evitar la publicidad no deseada’, ‘Cómo elaborar el registro de actividades de tratamiento’ y ‘Riesgos a los que puede enfrentarse la labor del DPD’ fueron los post que acumularon un mayor número de visitas.

▲ 2.3.3 Canal de YouTube

En enero de 2018 la Agencia dio un nuevo impulso estratégico a su canal de YouTube, gracias al cual el número de suscriptores experimentó un incremento de más del 160% en los once meses siguientes, hasta situarse en una cifra total de 1.783. Como consecuencia del rediseño de la página web de la web de la AEPD actualmente la Agencia publica la totalidad de sus vídeos en su canal de YouTube. Desde el comienzo de la nueva estrategia se han contabilizado casi 110.000 visualizaciones, los vídeos se han compartido en casi 4.000 ocasiones y se han registrado más de 700 ‘me gusta’.

▲ 2.3.4 Espacio ‘Protegemos tu privacidad’ de Radio 5

Gracias al acuerdo entre la AEPD y Radio 5 el espacio ‘Protegemos tu privacidad’ ofrece a los ciudadanos recomendaciones semanales para conocer sus derechos y saber cómo ejercerlos, así como consejos para facilitar el cumplimiento de la normativa a las organizaciones. La emisión comenzó el 4 de julio y a lo largo de 2018 se han emitido 25 piezas temáticas, en las que un experto de la Agencia ofrece consejos y recomendaciones. Además de la emisión todos los domingos a las 12.05 horas, los programas se encuentran disponibles en la página web de Radio 5.

▲ 2.3.5 Acuerdos con televisiones

La AEPD alcanzó en 2018 acuerdos para la emisión en diversos canales de contenidos relacionados con la protección de datos. A continuación, se detallan algunas de las iniciativas:

▲ **Clan TV. El valor de la privacidad y la importancia de luchar contra el ciberacoso**

La Agencia Española de Protección de Datos y Clan colaboraron para difundir entre los menores una campaña sobre el valor de la privacidad en Internet y la importancia de luchar contra el ciberacoso. La campaña, realizada en marzo de 2018, contó con seis vídeos editados a partir de materiales de la AEPD disponibles en la web 'Tuedecideseninternet.es' y en ellos se abordan cuestiones como el ciberacoso, la dependencia tecnológica o la huella digital, ofreciendo consejos y recomendaciones.

▲ **Boing. Tú decides en internet**

El canal para niños y adolescentes de Mediaset inició una campaña en julio de 2018 con la emisión de varios vídeos elaborados a partir de los materiales de la Agencia publicados en 'Tuedecideseninternet.es'. Partiendo de los aspectos positivos que conlleva un uso adecuado de internet, los vídeos abordaban también temáticas como la huella digital; el ciberacoso; la dependencia o el grooming.

▲ **Novedades del Reglamento, tanto para empresas como para los ciudadanos**

En 2018 se llevaron a cabo varias campañas divulgativas en televisión para difundir los derechos de los ciudadanos y las obligaciones para aquellos que tratan datos con la colaboración de la Comisión Nacional de los Mercados y la Competencia (CNMC), que declaró la campaña de la Agencia como exenta de cómputo publicitario.

Las campañas fueron difundidas por A3media, Mediaset y RTVE.

Fruto de estos acuerdos se emitieron, en las fechas previas y posteriores al 25 de mayo, los spots '¿Qué derechos tiene el ciudadano con la aplicación del RGPD?' y '¿Qué obligaciones tienen que cumplir las empresas ante la aplicación del RGPD? ¿Cómo puede ayudarme la Agencia?' en los canales Telecinco, Cuatro, FDF, Energy, Divinity y Be Mad, de Mediaset; Antena 3, La Sexta, Nova, Neox, Mega y Atreseries, de A3media, así como en La 1 y La 2 de RTVE. Sólo en Mediaset, la campaña tuvo más de 155 millones de impactos.

2018 fue el año del RGPD, por lo que gran parte de las consultas mediáticas tuvieron relación, de una forma u otra, con este nuevo marco normativo

▲ 2.3.6 Relaciones con los medios

Los medios de comunicación han seguido jugando un papel de vital importancia en lo que a protección de datos se refiere. Por una parte, favoreciendo la concienciación de los ciudadanos en relación con su derecho a la protección de datos y las novedades que incorpora el RGPD y, por otra, incrementando la sensibilización de los responsables del tratamiento de datos acerca de los mandatos que establece el nuevo contexto normativo europeo.

A lo largo de 2018, la Agencia atendió más de 770 consultas de medios de comunicación relacionadas con este derecho fundamental. Sin

duda, 2018 fue el año del Reglamento General de Protección de Datos, por lo que gran parte de las consultas recibidas tuvieron relación, de una forma u otra, con este nuevo panorama dispositivo.

De esta manera, la Agencia respondió numerosas peticiones de información vinculadas, por ejemplo, al grado de adecuación de las empresas en los meses previos al día 25 de mayo, fecha en que comenzó a aplicarse el RGPD.

Pero también hubo otras relacionadas con el posible incremento de recursos materiales y personales de la Agencia para hacer frente al previsible aumento de la carga de trabajo; la gran cantidad de correos electrónicos enviados por los responsables solicitando el consentimiento de los usuarios, o las implicaciones del Reglamento para los ciudadanos, en particular, los nuevos derechos o las novedades introducidas en la Ley Orgánica de Protección de Datos y garantía de los derechos digitales para incluir a una persona en los ficheros de solvencia patrimonial y crédito.

El Reglamento también suscitó consultas acerca de cómo afecta éste a distintos colectivos, como el de los informáticos, los detectives, o los profesionales del ámbito de la salud. Con carácter previo al día en que comenzó a aplicarse el Reglamento, la Agencia también recibió consultas de diversa temática, como las relacionadas con el derecho al olvido, el número de afectados por el caso Cambridge Analytica o la aplicación Grindr.

Con posterioridad al 25 de mayo, siguieron llegando un gran número de consultas relacionadas con el Reglamento. Por ejemplo, la solicitud de información sobre Delegados de Protección de Datos (DPD) y, en concreto, para aclarar cuándo es necesario contar con sus servicios ante los consejos de supuestos profesionales que recomiendan a pymes y autónomos disponer de un DPD cuando en realidad no era necesario. Asimismo, en los

meses siguientes se sucedieron las preguntas sobre la cantidad de reclamaciones recibidas por la AEPD y su temática.

En relación con otros ámbitos la Agencia resolvió dudas sobre cómo evitar la publicidad no deseada, el uso de videovigilancia o la posible afectación de usuarios españoles ante la brecha de seguridad de Facebook.

Esta labor de atención a los medios se vio complementada con la difusión de casi 300 notas de prensa, convocatorias y notas de agenda informativa publicadas en la web. En relación con estas últimas, la Agencia publicó en 2018 un total de 207 reuniones o actos públicos en los que participaron diferentes miembros de esta institución, cumpliendo un año más con la actuación prevista en Plan estratégico 2015-2019 de fomentar la publicación de su agenda institucional y ampliar sus contenidos para reforzar la transparencia.

2.4 Agenda Institucional

La asistencia del personal de la Agencia a reuniones institucionales y de trabajo, actos y jornadas experimentó un incremento de más del 17% con respecto a 2017. Esta agenda se puede consultar de manera cronológica en la sección Agenda de la página web de la AEPD.

El año 2018 fue especialmente intenso en lo que respecta a la organización de jornadas, encuentros y sesiones informativas, acciones formativas, talleres, actos y presentaciones por parte de la Agencia. Este conjunto de acciones tuvo como objetivo explicar las novedades del Reglamento General de Protección de Datos, así como facilitar la adaptación al mismo tanto del sector público como privado.

La Agencia ha desarrollado con intensidad una actuación formativa, dirigida especialmente al sector público, así como la de acompañamiento

a los responsables y encargados del tratamiento para facilitar el cambio de modelo.

Dentro del capítulo de actividades públicas organizadas por la Agencia se encuentran, entre otros ejemplos, las Jornadas para la adaptación del RGPD en las Administraciones Públicas, en las Comunidades Autónomas, y en la Administración Local; las presentaciones de las Guías de Análisis de Riesgo y Evaluación de Impacto en la Protección de los Datos, de Protección de Datos y Prevención del Delito, y para la Gestión y Notificación de Brechas de Seguridad, o el Acto de celebración del 25 aniversario de la AEPD.

Por otra parte, la Agencia organizó talleres informativos sobre el RGPD dirigidos específicamente a sectores estratégicos de la economía nacional -energético, turismo, gran consumo o publicidad-, así como talleres de aplicación práctica del Reglamento dirigidos a Delegados de Protección de Datos de la Administración General del Estado, de las Comunidades Autónomas o las Diputaciones Provinciales.

Asimismo, continuó con su participación en jornadas sobre el RGPD en los Institutos o Escuelas de formación de Administración Pública de varias Comunidades Autónomas y mantuvo reuniones con diversos organismos públicos, como el Consejo General del Poder Judicial; la Comisión Nacional de los Mercados y la Competencia; la Autoridad Catalana de Protección de Datos; la Agencia Vasca de Protección de Datos; el Centro Criptológico Nacional, o con representantes de otros como el Ministerio de Justicia; el Tribunal de Cuentas; Red.es; la Dirección General de Tráfico; la Administración Periférica del Estado, o la Junta Electoral Central.

En el ámbito del sector privado, la Agencia Española de Protección de Datos desarrolló jornadas sobre las implicaciones del RGPD en las confederaciones empresariales de varias Comunidades Autónomas y participó

en numerosos actos como, entre otros, la Jornada sobre el RGPD en el sector asegurador, organizado por la Asociación Empresarial del Seguro (UNESPA); el Foro SEDISA-ALSEDISA sobre calidad y sostenibilidad; el XV Foro de Seguridad y Protección de Datos en Salud organizada por la Sociedad Española de Informática de la Salud; la Jornada en la Confederación Nacional de Autoescuelas; la Jornada 'Compliance y protección de datos', organizada por la Federación Nacional de Consultoría y Servicios Profesionales (FENAC) y la Confederación Española de la Pequeña y Mediana Empresa (CEPYME); la Jornada sobre el 'Reglamento Europeo de Protección de Datos: Aplicación en el Sector Sanitario', organizada por la Alianza de la Sanidad Privada Española (ASPE); la Jornada sobre el RGPD en la Asociación Empresarial del Seguro (UNESPA); la Jornada sobre el 'Impacto de la nueva normativa de protección de datos en las empresas y organizaciones empresariales', celebrada en la Confederación Española de Organizaciones Empresariales (CEOE); el IV Congreso Internacional de Derecho Digital, organizado por la Asociación de Expertos Nacionales de la Abogacía Tecnológica (ENATIC); el XII Foro de la Asociación Española de Profesionales del Turismo (AEPT); el XXI Congreso Nacional Consejo General de Colegios de Administradores de Fincas de España (CGCAFE); la II Jornada Anual sobre protección de datos y Abogacía, organizada por el Consejo General de la Abogacía Española; el Seminario sobre el impacto de la nueva regulación de protección de datos en la investigación biomédica, organizado por el Centro de Estudios para el Fomento de la Investigación (CEFI); la Jornada 'Ciberseguridad y primeros meses de GDPR: Avanzando en la gestión segura del dato', organizada por la Asociación para el Progreso de la Dirección (APD); la Jornada 'Cuestiones relativas a la Seguridad en el colectivo de Administradores de Fincas', organizada por el Consejo General de Colegios de Administradores de Fincas; el VII Congreso de Regulación Publicitaria Digital, organizado por IAB Spain, o el Foro de la Gobernanza de Internet en España (IGF Spain).

Además, mantuvo reuniones con representantes de la Asociación Digitales; la Asociación para la Autorregulación de la Comunicación Comercial (Autocontrol); la Confederación Española de la Pequeña y Mediana Empresa (CEPYME); la Asociación para el Progreso de la Dirección (APD); la Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS); la Sociedad Española de Epidemiología (SEE); la Asociación Profesional Española de Privacidad (APEP); la Asociación Española de la Economía Digital (ADigital); la Federación de Asociaciones Científico Médicas Españolas (FACME); el Consejo de Consumidores y Usuarios; la Interactive Advertising Bureau (IAB Spain); la Conferencia Episcopal; la Red Española del Pacto Mundial; la Asociación de Empresas y Profesionales de la Responsabilidad Social Empresarial (Forética), o la Asociación de Fabricantes y Distribuidores, entre otras.

Finalmente, El Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia- se reunió el 24 de enero y el 12 de julio de 2018 para exponer y analizar la actividad de la institución. En la primera de las reuniones, el Consejo abordó las actividades más destacadas de la institución realizadas en 2017, y se falló la vigésimo primera edición de los Premios Protección de Datos. En la segunda, se expusieron las acciones realizadas en el primer semestre de 2018.

2.5 Página web

La página web de la Agencia registró más de 7,9 millones de visitantes únicos en 2018

Con la vista puesta en el 25 de mayo, la Agencia continuó trabajando para dar a conocer las implicaciones del Reglamento

General de Protección de Datos a ciudadanos y responsables, a través de sus guías, informes, infografías, vídeos y otros materiales, y habilitando nuevos servicios para facilitar esta tarea.

En paralelo, la Agencia trabajó intensamente en los meses previos al 25 de mayo para rediseñar completamente la página web de la Agencia y adaptar todos los contenidos y estructura conforme al nuevo marco normativo europeo.

Entre estas iniciativas se encuentra la publicación en la página web de la Agencia de los vídeos de la celebración de una jornada de formación sobre **‘El RGPD y las implicaciones para la Administración Local’**, organizada junto a la Federación Española de Municipios y Provincias (FEMP). En la jornada se analizaron, entre otros aspectos, las actuaciones de la AEPD para facilitar el cumplimiento del RGPD, el impacto del Reglamento en las Administraciones Locales y la figura del Delegado de Protección de Datos.

Con motivo de la celebración del Día europeo de Protección de Datos el 28 de enero, marcada por el RGPD, la Agencia publicó una infografía con los **nuevos derechos de los ciudadanos** a partir del 25 de mayo. Desde esta fecha se puede acceder a esta infografía a través de una sección propia en la página web de la Agencia.

Por otra parte, la Agencia dio especial relevancia a la publicación de un informe en el que, ante la preocupación manifestada en diversos foros por las sociedades científicas, examinaba la incidencia en el ámbito de la investigación biomédica del Reglamento y el Proyecto de LOPD.

Asimismo, publicó **‘Utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas’**, un informe basado en un estudio realizado entre centros educativos en colaboración con asociaciones del sector para recabar datos de estos centros

sobre cómo emplean este tipo de aplicaciones y herramientas. El estudio recaba información sobre el uso que alumnos y profesores hacen de herramientas de almacenamiento en nube, redes sociales y correo electrónico, al margen de las plataformas educativas de los centros y a iniciativa de los profesores. Sólo algunos centros han declarado haber establecido normas internas para autorizar su uso.

Además, la Agencia publicó el estudio '**Políticas de privacidad en Internet. Adaptación al RGPD**', para examinar la adaptación de las empresas al RGPD en sus políticas de privacidad online, así como dictar recomendaciones para su correcta aplicación. La publicación de este informe se acompaña de un Decálogo que recoge los aspectos más relevantes que deben tener en cuenta los responsables para dar cumplimiento al RGPD, como informar sobre quién trata los datos, con qué finalidad, qué base legal legitima el tratamiento, cuánto tiempo se conservan, los derechos de los usuarios y cómo ejercerlos, si los datos se van a ceder a terceros, si se toman decisiones automatizadas o si se van a realizar transferencias internacionales, entre otros.

La publicación de contenidos se vio complementada en 2018 con la puesta en marcha de varios servicios para ayudar en el proceso de adaptación al Reglamento.

La Agencia puso en marcha en su Sede electrónica un procedimiento para que las Administraciones Públicas y las entidades privadas pudieran comunicar el nombramiento del Delegado de Protección de Datos

También publicó el **Listado de cumplimiento normativo** -un documento con el que las organizaciones pueden identificar y verificar que están teniendo en cuenta los requerimientos establecidos por el nuevo RGPD- o registro de actividades de tratamiento de la Agencia con el objetivo de mostrar de forma transparente cómo puede elaborarse este registro en caso de tratamientos complejos o Administraciones Públicas. El espíritu de esta publicación es ayudar a otros responsables a encontrar respuesta a su búsqueda de un ejemplo de cómo cumplir con esta obligación, aunque el principio de responsabilidad activa recogido en el Reglamento General de Protección de Datos (RGPD) deja a cada responsable la decisión de cómo implementarlo.

Asimismo, publicó el **registro de Delegados de Protección de Datos (DPD)** que, a 31 de diciembre, contiene los datos de contacto más de 20.000 entidades, de las cuales alrededor de 3.000 corresponden al sector público y las restantes al sector privado. Este espacio de consulta, disponible en la Sede electrónica de la Agencia, permite a cualquier interesado conocer el contacto de los delegados de protección de datos comunicados a la AEPD. De esta forma, los ciudadanos que quieran ejercitar sus derechos o presentar una reclamación ante una entidad pueden introducir el nombre, razón social o NIF de la organización para conocer los datos de contacto del DPD y dirigirle sus solicitudes.

La Agencia publicó también varias **infografías de temática variada**. Entre ellas, las destinadas a evitar la publicidad no deseada; los nuevos derechos del RGPD; recomendaciones para la compra de juguetes conectados; consejos para comprar de forma segura en internet, y la adaptación al Reglamento de Administraciones Públicas y el sector privado.

2.6 Actividades de divulgación: Guías y Herramientas al servicio de los Responsables

La AEPD participó en 2018 en numerosas jornadas, seminarios, mesas redondas, cursos y charlas informativas para expandir la cultura de protección de datos entre los ciudadanos y organizaciones. En este sentido, continuó con su iniciativa emprendida en 2017 de celebrar jornadas de formación sobre las novedades del RGPD en centros o institutos de formación autonómicos de las Comunidades Autónomas y en organizaciones empresariales a escala autonómica.

A estas hay que añadir diversas acciones de divulgación.

▲ Presentación de las Guías de Análisis de riesgos y Evaluaciones de Impacto

El 28 de febrero de 2018 la Agencia presentó la Guía de Análisis de Riesgos y la Guía de Evaluación de Impacto en la Protección de Datos en un acto celebrado con asociaciones empresariales de los sectores de la banca, energía, gran consumo, seguros, publicidad y turismo, entre otros, y representantes de las Administraciones Públicas.

▲ Presentación de la Guía 'Protección de Datos en la Administración Local'

El 3 de abril tuvo lugar la presentación de la Guía Protección de datos y Administración Local en un acto celebrado con representantes de la Federación Española de Municipios y Provincias (FEMP) y del Consejo General de Secretarios, Interventores y Tesoreros de Administración Local (COSITAL), y contó con la presencia de representantes de ayuntamientos y diputaciones provinciales.

▲ Presentación del manual 'Protección de Datos y prevención de delitos'

El 10 de mayo se presentó el manual Protección de Datos y Prevención de delitos en un acto conducido por la directora de la Agencia en el que también participó la fiscal de Sala coordinadora en materia de Criminalidad Informática, Elvira Tejada. El objetivo de este documento es ofrecer información sobre las consecuencias de la difusión no consentida de información personal a través de servicios online, así como proporcionar pautas tanto para no incurrir en conductas que podrían ser constitutivas de delito como para no ser víctima de ellas.

▲ 10ª Sesión Anual Abierta de la AEPD

El 4 de junio la AEPD celebró su 10ª Sesión Anual Abierta, un encuentro que contó con la asistencia de más de 600 personas y pudo seguirse en directo en streaming a través de la web de la Agencia, con más de 5.000 visitas. La Sesión -dirigida a representantes de instituciones, empresarios y profesionales de la protección de datos- se centró en efectuar un repaso por las implicaciones prácticas del RGPD y las iniciativas de adaptación al mismo, haciendo especial hincapié en herramientas como Facilita_RGPD -para empresas que traten datos de bajo riesgo- y las guías de análisis de riesgos y evaluación de impacto en la protección de datos.

En la Sesión también se analizaron otros temas, como el gran volumen de comunicaciones enviadas a los ciudadanos en los días previos al 25 de mayo que solicitaban el consentimiento; los códigos de conducta, o el régimen sancionador, incidiendo en la existencia de medidas como la advertencia o el apercibimiento que pueden adoptarse en lugar de una sanción económica cuando, pese a producirse un error, se aprecie y documente una adecuada diligencia en el cumplimiento del RGPD.

▲ Entrega de los Premios Protección de Datos 2017

La Agencia Española de Protección de Datos (AEPD) entregó durante la celebración de su 10ª Sesión Anual Abierta los ‘Premios Protección de Datos 2017’ en las categorías de Comunicación, Investigación, Adaptación al Reglamento y Buenas prácticas en centros escolares. Estos galardones reconocen los trabajos que promueven en mayor medida la difusión y el conocimiento del derecho fundamental a la protección de datos, así como su aplicación práctica en diferentes entornos.

El jurado –compuesto por el Consejo Consultivo de la AEPD– concedió el premio principal de comunicación al periodista Pedro del Rosal, por las noticias, reportajes y entrevistas publicadas en El Economista sobre la aplicación del RGPD y la adaptación al nuevo marco normativo, entre otros temas. Asimismo, otorgó un accésit a Carlos Fernández, del Diario La Ley, por las informaciones publicadas en referencia a, entre otros aspectos, el Reglamento, las obligaciones de las Administraciones Públicas ante la nueva normativa y las directrices de las Autoridades europeas para adaptarse al nuevo contexto.



En la categoría de ‘Buenas prácticas en privacidad y protección de datos personales sobre iniciativas para adaptarse al Reglamento europeo de Protección de Datos’, en la modalidad de empresas, asociaciones y fundaciones, el jurado concedió el premio a la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA), por las acciones e iniciativas realizadas. En el apartado de entidades del sector público, se otorgó el premio a la Gerencia de Informática de la Seguridad Social, por su propuesta para la adecuación al RGPD desde el rol de encargado del tratamiento.

Respecto al Premio a las ‘Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet’, el jurado concedió el premio en la modalidad dirigida a centros de enseñanza públicos, concertados y privados de Educación Primaria, Educación Secundaria Obligatoria, Bachillerato y Formación Profesional, al IES Isaac Albéniz de Leganés (Madrid), por su trabajo ‘Uso y Abuso de las redes sociales y su implicación en el entorno educativo’.

En relación con la modalidad que reconoce el compromiso de personas, instituciones, organizaciones y asociaciones, públicas y privadas que hayan destacado por el impulso y difusión entre los menores de edad de buenas prácticas para un uso seguro de internet, el jurado otorgó el premio a la Policía Nacional y la Guardia Civil, por la ejecución del ‘Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos’.

Finalmente, en la categoría de ‘Investigación en protección de datos personales Emilio Aced’ el jurado otorgó el premio principal a Abel Lozoya de Diego por su trabajo ‘Modelo de atributos clínicos a anonimizar para el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal’. Asimismo, concedió el

accesit a Santiago Saavedra, Sofía Prósper, Guidiana Landívar y Alba Martín –con la colaboración de Pablo Martín, Carla Tortul, Adolfo Antón y Medialab-Prado- por su trabajo ‘Trackula’.

▲ Encuentro informativo en la Asociación de Comunicadores e informadores jurídicos (ACIJUR)

El 6 de junio tuvo lugar un encuentro con periodistas en la sede de la Mutualidad de la Abogacía en el que la directora de la AEPD contestó a las preguntas sobre la aplicación del nuevo Reglamento General de Protección de Datos (RGPD) y las actuaciones realizadas por la Agencia.

▲ Presentación Guía de quiebras de seguridad

El 19 de junio, la AEPD presentó la ‘Guía para la gestión y notificación de brechas de seguridad’, realizada junto a ISMS Forum y en colaboración con el Centro Criptológico Nacional (CCN) e INCIBE. El objetivo de este documento es ofrecer a las organizaciones tanto recomendaciones preventivas como un plan de actuación, de forma que conozcan cómo evitarlas y cómo proceder en caso de que se produzcan.

▲ Presentación Encuesta ‘Grado de preparación de las pymes españolas ante el RGPD’

El 19 de julio, la AEPD y CEPYME presentaron los resultados de una encuesta realizada entre las pymes españolas para conocer la percepción y el grado de conocimiento del nuevo Reglamento General de Protección de Datos. La encuesta se enmarca en el ámbito del protocolo de colaboración suscrito entre estas entidades y de la voluntad de ambas partes de conocer la realidad de las pymes españolas para seguir realizando acciones de información y difusión que impulsen el cumplimiento.



▲ Acto conmemorativo del 25 aniversario de la AEPD

El 13 de noviembre de 2018, la AEPD celebró en el Senado una jornada para conmemorar su 25 aniversario, un acto que fue inaugurado por el presidente del Senado, Pío García-Escudero, la ministra de Justicia, Dolores Delgado, y la directora de la Agencia, y que contó con la participación de los directores anteriores y representantes de organismos internacionales de protección de datos.

Durante la jornada se presentó el libro ‘25 años de la AEPD: acompañando al ciudadano en su transformación digital’, que describe la evolución de la sociedad española en conexión con la historia, hitos y actividad de la Agencia desde sus comienzos en 1993, así como el desarrollo de este derecho fundamental.

Los vídeos de cada una de las intervenciones de la jornada pueden visualizarse desde este [enlace](#).

▲ Recomendaciones para fomentar la compra segura en internet y juguetes conectados

El 19 de noviembre, la Agencia, la Dirección General de Política Comercial y Competitividad, y la Dirección General de Consumo celebraron un acto en la sede de la AEPD en el que ofrecieron recomendaciones para fomentar la compra segura en internet, incluyendo consejos específicos sobre juguetes conectados. Esta presentación tuvo lugar pocos días antes del Black Friday y el Cyber Monday –23 y 26 de noviembre, respectivamente–, fechas elegidas por millones de personas para adquirir productos de todo tipo y, en muchos casos, para anticipar sus compras navideñas.

▲ Encuentro informativo sobre la nueva Ley Orgánica de Protección de Datos y garantía de derechos digitales

El 22 de noviembre se celebró un encuentro con periodistas para informar sobre la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, que se aprobó por unanimidad en el Congreso de los Diputados y con un 92% de apoyo en el Senado. La nueva normativa, que adapta el derecho español al modelo establecido por el RGPD, introduce novedades mediante el desarrollo de materias contenidas en el mismo.

2.7 Premios recibidos por la AEPD

El 25 de abril tuvo lugar la entrega de los ‘XV Premios de Seguridad de la Información de la Revista SIC’, que concedió un Premio SIC a la AEPD “en reconocimiento a la labor que viene realizando desde hace años, fuera y dentro de España, para promover el conocimiento de los derechos a la privacidad y a la protección de datos personales y para facilitar el cumplimiento de la legislación en la materia”.

El 17 de mayo de 2018 la asociación de Expertos Nacionales en Abogacía Tecnológica (Enatic) celebró su gala anual de entrega de premios, entregando el Premio Enatic de Honor -reservado a personalidades que hayan contribuido de forma extraordinaria al avance del Derecho digital- ex æquo, a Mar España y Jesús Rubí, directora y adjunto a la dirección de la AEPD, respectivamente, “por el impulso y el liderazgo que ejercen desde esta Institución, especialmente en ámbitos como la comunicación y divulgación, la elaboración de documentos técnicos de gran calidad y la rápida reacción ante flagrantes vulneraciones de la protección de datos personales”.

También en mayo, la organización X1RedMasSegura otorgó una mención honorífica de sus ‘Premios 2018’ a la Agencia Española de Protección de Datos “en agradecimiento por su inestimable labor y encomiable esfuerzo en aras de llevar la protección de datos, la seguridad y la educación en la red a los colectivos más vulnerables”.

2.8 Transparencia y Compliance

Durante el año 2018 se ha actualizado la información que se publica en esta sección de la web de la AEPD, denominada ‘Transparencia’, que fue creada en cumplimiento de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, y cuya finalidad es facilitar a los ciudadanos de una forma clara y ordenada todos los contenidos de publicidad activa que regula la citada Ley.

El canal de transparencia se muestra dividido en cuatro grandes apartados, mostrando en cada uno de ellos, respectivamente, datos de Información institucional, organizativa y de planificación; Información de relevancia jurídica; Información económica, presupuestaria y estadística y otro tipo de información. En este último apartado se incluye la información relativa a la agenda institucional,

a la sesión anual abierta de la AEPD y el registro de actividades de tratamiento. Esta sección de la web recibió un total de 421.485 visitas en el año 2018.

Por lo que respecta al acceso a la información pública, en 2018 se recibieron 118 solicitudes, frente a las 59 de 2017, es decir, se han doblado en número. De ellas, se atendieron 84, se inadmitieron 7 y 3 fueron denegadas.

Sobre las inadmisiones, cabe señalar que se motivaron en la aplicación del artículo 18 de la Ley 19/2013: abuso de derecho, información pendiente de publicación e información que no obra en poder de la AEPD. Por último, es preciso indicar que, de las 118 solicitudes, 24 fueron tramitadas y resueltas como consultas y no como solicitudes de acceso a la información, aunque se recibieran a través del Portal de Transparencia.

El artículo 36.1 f) de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno (LTAIBG), establece que integrará la Comisión de Transparencia y Buen Gobierno un representante de la Agencia Española de Protección de Datos, habiendo sido designado en representación de la Agencia el Abogado del Estado - Jefe del Gabinete Jurídico.

La función de la Agencia en esta materia no se limita a la participación del miembro de la Comisión designado por aquélla en los trabajos de la misma, sino que además, de conformidad con lo establecido en la disposición adicional quinta, corresponderá de forma conjunta a la Agencia y al Consejo de Transparencia y Buen Gobierno la adopción conjunta de los criterios de aplicación de las reglas contenidas en el artículo 15 de la propia Ley, “en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma”.

A lo largo de 2018 se han celebrado cinco reuniones de la Comisión.

Por otra parte, el artículo 24 de la LOPDGDD, impulsado por la Agencia, ha regulado los sistemas de información de denuncias internas para poner en conocimiento de entidades privadas, incluso anónimamente, la comisión en su ámbito interno o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial aplicable. Adicionalmente, este precepto incorpora garantías sobre el acceso a dichas informaciones y la conservación de las mismas.

Esta iniciativa manifiesta el compromiso de la Agencia en la lucha contra la corrupción y en favor de la transparencia, frente aquellos que utilizan la normativa de protección de los datos personales como excusa para evitar combatirla.

Esta iniciativa de impulsar la regulación de sistemas de información de denuncias internas manifiesta el compromiso de la Agencia en la lucha contra la corrupción y en favor de la transparencia

➤ 3. Ayuda efectiva para las entidades

3.1 El Registro General de Protección de Datos

La aplicación del RGPD ha puesto punto final a la obligación de notificar a las autoridades de control los ficheros que mantenían las organizaciones y que, con carácter general, les suponía el primer contacto con la materia de protección de datos.

El 14 de mayo de 2018 se deshabilitó el sistema de notificación de ficheros mediante los formularios de la Sede Electrónica de la Agencia y el Registro General de Protección de Datos dejó de estar operativo.

A dicha fecha, el Registro General de Protección de Datos contaba con 5.094.313 ficheros inscritos, de los que 168.499 eran de titularidad pública y 4.925.814 de titularidad privada. No obstante, entre el 1 de enero y su cierre, el Registro General de Protección de Datos desarrollo una amplia actividad, el número de operaciones diarias realizadas se mantuvo en 2.541, lo que supuso un incremento de 1.794 ficheros inscritos diariamente.

▲ 3.1.1 Transferencias internacionales

La aplicación del RGPD también afectó profundamente a la regulación de las transferencias internacionales al suprimirse, con carácter general y como consecuencia de la aplicación del principio de responsabilidad proactiva en su cumplimiento, tanto la obligación de notificar las transferencias internacionales de datos al Registro General de Protección de Datos que, como se ha indicado, dejó de estar operativo, como la de obtener la autorización previa de la Agencia para llevarlas a cabo en los casos en los que se aportasen de garantías adecuadas, ya fuese mediante contratos o normas corporativas vinculantes (BCR) en los casos de grupos empresariales multinacionales.

Al cierre del Registro General de Protección de Datos se habían concedido 2.169 autorizaciones para realizar transferencias internacionales de datos, de las que 443 correspondían a transferencias entre responsables del tratamiento, 1.590 a transferencias entre responsable y encargados, 48 entre encargados del tratamiento y 88 entre entidades de grupos empresariales que disponían de normas corporativas vinculantes (BCR).

Durante 2018, hasta la fecha de aplicación del RGPD, se autorizaron 78 transferencias internacionales de datos.

Los países de destino de los datos que han dado lugar a un mayor número de autorizaciones han sido: Estados Unidos (966), India (356), Colombia (176), Perú (155) y México (102).

El Registro General de Protección de Datos se ha mantenido, no obstante, en el estado de desarrollo que se encontraba en el momento de su cierre al objeto de atender las solicitudes de copia de contenido de la inscripción de los ficheros que los responsables de los tratamientos presenten, en la medida que les puede servir de ayuda para la elaboración del registro de actividades de tratamiento, y que en 2018 ascendieron a 12.819, que fueron atendidas en una media de 4 a 7 días.

3.2 El Registro de Delegados de Protección de Datos

El artículo 37.7 del Reglamento General de Protección de Datos establece que el responsable o encargado de tratamiento debe comunicar a la autoridad de control los datos de su delegado de protección de datos. Con fecha 9 de abril de 2018, la Agencia Española de Protección de Datos habilitó en su Sede Electrónica un nuevo formulario para la recepción de las comunicaciones que responsables y encargados habían comenzado a realizar. A fecha 31 de diciembre de 2018, el número de responsables y encargados que habían realizado la comunicación de su delegado de protección de datos era de 20.048, de ellos 2.752 correspondían al denominado sector público (autoridades y organismos públicos) y 17.296 a entidades privadas.

Así mismo, la Agencia puso en funcionamiento el 4 de diciembre, 3 días antes de la entrada en vigor de la LOPDGD, un sistema de consulta electrónica de los delegados de protección de datos que le han sido comunicados, a través de la denominación del responsable y/o su NIF.

3.3 Códigos de Conducta

Los códigos tipo, de acuerdo con la denominación utilizada por la Directiva 95/46 y la LOPD y su reglamento de desarrollo, o códigos conducta, de acuerdo con el término utilizado en el RGPD, son una manifestación de iniciativas de autorregulación.

En el marco de esta autorregulación que el Reglamento Europeo de Protección de Datos promueve y fomenta, los códigos de conducta, junto con las certificaciones, destacan como una herramienta útil para demostrar que responsables y encargados cumplen con los requisitos establecidos en el mismo. Son instrumentos que obedecen al principio de responsabilidad proactiva.

El objetivo principal del RGPD al dar una mayor relevancia a los códigos de conducta es que sirvan como herramientas para que los responsables y encargados puedan demostrar su cumplimiento, teniendo en cuenta las características y necesidades específicas de los distintos sectores de actividad y, en particular, de las pymes y micropymes. Para ello, señala a los Estados miembros, las autoridades de protección de datos, el Comité Europeo de Protección de Datos, así como a la Comisión Europea, como impulsores para la elaboración de códigos de conducta por las asociaciones y otros organismos representativos de categorías de responsables y encargados del tratamiento, así como para la adaptación de los ya existentes por parte de sus promotores. El doble marco normativo aplicable durante 2018 ha dado lugar a que la Agencia haya tramitado solicitudes de códigos tipo y solicitudes de aprobación de códigos de conducta al amparo de las previsiones del RGPD.

Códigos Tipo en el marco de la Ley Orgánica 5/1999 (LOPD):

Se han tramitado cuatro solicitudes de inscripción de códigos tipo que dieron lugar a una resolución de archivo y a la inscripción de los siguientes códigos tipo:

- ▲ CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
- ▲ CÓDIGO DE CONDUCTA PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR ORGANIZACIONES DE INVESTIGACIÓN DE MERCADOS, SOCIAL Y DE LA OPINIÓN Y DEL ANÁLISIS DE DATOS, promovido por la Asociación Nacional de Empresas de Investigación de Mercados y Opinión Pública (ANEIMO) y la Asociación Española de Estudios de Mercado, Marketing y Opinión (AEDEMO)

▲ CÓDIGO TIPO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DE LA ASOCIACIÓN ESPAÑOLA DE MICROPRÉSTAMOS

Códigos tipo que, conforme dispone la Disposición Transitoria Segunda de la LOPDGDD, disponen de un año, a contar desde el pasado 7 de diciembre de 2018, para adaptar su contenido a lo dispuesto en el artículo 40 del RGPD. Transcurrido dicho plazo sin haber procedido a solicitar la aprobación de su adecuación al RGPD se cancelará la inscripción y se comunicará a sus promotores.

Códigos de conducta en el marco del Reglamento General de Protección de Datos (RGPD):

Durante el año 2018 se han presentado formalmente dos solicitudes de aprobación de proyectos de códigos de conducta que a 31 de diciembre de 2018 se encontraban en tramitación:

▲ CÓDIGO DE CONDUCTA SECTOR INFOMEDIARIO PROTECCIÓN DE DATOS, promovido por la Asociación Multisectorial de la Información (ASEDIE).

▲ CÓDIGO CONDUCTA DE TRATAMIENTO DE DATOS EN LA ACTIVIDAD PUBLICITARIA, promovido por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL), cuyo objeto es el establecimiento de un procedimiento extrajudicial de resolución de controversias entre las entidades adheridas al Código y los interesados.

Se devolvió el proyecto de CÓDIGO DE CONDUCTA ASOCIACIÓN ESPÍRITA OTUS I NERAM, presentado ante la Autoridad Catalana de Protección de Datos, y se informó a sus promotores de los requisitos que son necesarios para solicitar formalmente su aprobación.

La aplicación del RGPD y las acciones llevadas

a cabo por la Agencia Española de Protección de Datos para la promoción de los códigos de conducta ha despertado interés en diferentes sectores de actividad que se ha plasmado en las siguientes iniciativas de códigos de conducta que a finales de 2018 no habían dado lugar a una presentación formal:

▲ CÓDIGO DE CONDUCTA SOBRE ATENCIÓN Y MEDIACIÓN DE DERECHOS EN PROTECCIÓN DE DATOS, promovido por la Asociación Española de Economía Digital (ADIGITAL)

▲ CODIGO DE CONDUCTA DEL SERVICIO DE LISTA ROBINSON, promovido por ADIGITAL

▲ CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES KUMON, promovido por Kumon Instituto de Educación de España (KUMON)

▲ CÓDIGO DE CONDUCTA PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIÓN DE FEDERACIONES DEPORTIVAS MADRILEÑAS, promovido por la Unión de Federaciones Deportivas Madrileñas (UFEDEMA)

▲ CÓDIGO DE CONDUCTA AGENCIAS DE VIAJES, promovido por la UNIÓN AGENCIAS VIAJES

▲ CÓDIGO DE CONDUCTA DE COLEGIO DE INGENIEROS DE TELECOMUNICACIONES, promovido por el COLEGIO DE INGENIEROS DE TELECOMUNICACIONES

▲ CÓDIGO DE CONDUCTA DE ORANGE, promovido por ORANGE

Asimismo, se han mantenido reuniones y conversaciones con los promotores de los siguientes códigos tipo para su adaptación al RGPD como códigos de conducta:

▲ CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

▲ CÓDIGO ÉTICO DE CONFIANZA ONLINE

3.4 Recursos para facilitar el cumplimiento del RGPD

La Agencia, con la finalidad de que puedan servir de orientación a los responsables de los tratamientos de datos y facilitarles las tareas de adecuación al régimen del RGPD, hizo público su registro de actividades de tratamiento, las cláusulas que utiliza para dar cumplimiento al derecho de información de los ciudadanos cuyos datos personales son objeto de tratamiento por la Agencia en sus diversas actividades y un modelo de cláusula para contratos con encargados del tratamiento.

3.4.1 Canal INFORMA

El Plan Estratégico recoge dentro del eje de actuación relativo a “Una Agencia cercana a los responsables y a los profesionales de la privacidad” la relación con los sujetos obligados que tiene entre sus objetivos el de contribuir a resolver las dudas que genera el cumplimiento de la normativa de protección de datos. Con motivo de la aplicación del RGPD, el 1 de marzo se puso en marcha el canal INFORMA_RGPD para ayudar a resolver aquellas cuestiones, dudas o incertidumbre que puedan derivarse de su cumplimiento.

El canal está disponible para:

- ▲ Los responsables y encargados de tratamientos, a través de la persona que ostente su representación.
- ▲ Los delegados de protección de datos. Si han nombrado un delegado de protección de datos, ya sea obligatorio o facultativo, será éste quien deba plantear las preguntas y dudas.
- ▲ Las Administraciones Públicas, a través de sus correspondientes delegados de protección de datos.
- ▲ Las organizaciones y asociaciones representativas de categorías de responsables y/o encargados del tratamiento.

Desde su puesta en funcionamiento y hasta el 31 de diciembre de 2018, ha recibido un total de 4.116 consultas sobre diversas cuestiones, entre las que cabe destacar:

- ▲ Las relativas a la designación de delegado de protección de datos y cuándo es obligatorio, desde diferentes sectores de actividad: sanitario, educativo, profesionales, etc.
- ▲ La videovigilancia: comunidades de propietarios, piscinas, taxis, autobuses, etc.
- ▲ Las relativas a la huella dactilar y otros datos biométricos y su tratamiento para fines de control de acceso y horario del trabajo.
- ▲ La prevención de riesgos laborales y los cambios de empresas encargadas de la prevención.
- ▲ Las medidas de seguridad, en especial, los softwares.
- ▲ El artículo 28.2 de la ley 39/2015, antes de su modificación llevada a cabo por la LOPDPGDD.
- ▲ La notificación de brechas de seguridad.
- ▲ Los plazos de conservación de los datos en diferentes entornos.
- ▲ El papel del responsable y encargado del tratamiento, por los colectivos como los de Procuradores de los Tribunales y Auditores de Cuentas.
- ▲ El uso de aplicaciones de mensajería instantánea entre profesionales y clientes en diferentes entornos.

3.4.2 Actividades de divulgación

La aplicación del RGPD ha supuesto una intensa labor de difusión entre todos los sectores implicados que la Agencia Española de Protección de Datos viene desarrollando desde 2017, en correspondencia con las funciones que le atribuye el propio RGPD para la promoción y sensibilización entre responsables y encargados del tratamiento de las obligaciones que establece.

PROTOCOLO CON UNIÓN PROFESIONAL

El 14 de marzo se suscribió un protocolo de colaboración para dar a conocer y difundir entre las corporaciones colegiales y sus miembros las herramientas, métodos, disposiciones y cualquier otro material de la Agencia que sean de interés para el cumplimiento de la normativa de protección de datos, la participación en sesiones y jornadas de formación.

La colaboración de la Agencia con Unión Profesional, que agrupa a 33 Consejos y Colegios Generales, constituye uno de los cauces habituales para atender y apoyar al colectivo de profesionales sujetos a colegiación en el cumplimiento del RGPD.

CONVENIO CON CEPYME

EL 30 de abril se firmó un convenio de colaboración con CEPYME que tenía por objeto la realización de un estudio sobre el grado de conocimiento, preparación y adaptación de las PYMES al RGPD, con el objetivo de planificar y adoptar las medidas más adecuadas según las necesidades que se detecten en la adaptación y cumplimiento de las obligaciones que establece el citado Reglamento.

PROTOCOLO CON LA ASOCIACIÓN ESPAÑOLA DE COMPLIANCE (ASCOM)

Los profesionales que integran ASCOM desempeñan un papel importante en el cumplimiento de la normativa de protección de datos de los responsables a los que prestan sus servicios. El interés de ASCOM por todo lo relacionado con la protección de datos

para el ejercicio de la función de Compliance llevó a la firma, el 13 de marzo, de protocolo de colaboración con la principal finalidad de facilitarle a ASCOM los materiales, herramientas y contenidos que a los efectos indicados sean de utilidad para sus asociados.

PLAN DE DIFUSIÓN DEL RGPD

Como se ha enunciado en otros apartados de esta Memoria, la Agencia ha continuado con las acciones de concienciación, información y formación mediante diferentes actividades dirigidas tanto del sector público como privado.

La relación de actividades que durante 2018 se han llevado a cabo para la difusión del del RGPD y de las novedades que su aplicación comporta a los distintos sectores de actividad, privados y públicos, así como a mostrar y difundir la herramienta FACILITA es la siguiente:

09/04/2018	Encuentro informativo sectorial sobre el RGPD “Grandes superficies de distribución y consumo”
19/04/2018	Encuentro informativo sectorial sobre el RGPD “Turismo”
24/04/2018	Jornada Informativa para las PYMES sobre el RGPD (Mallorca)
24/04/2018	Jornada Informativa para el sector privado sobre el RGPD (Barcelona)
25/04/2018	Encuentro informativo sectorial sobre el RGPD “Energía – Asociación Española de la Industria Eléctrica UNESA”
03/05/2018	Jornada Informativa para las PYMES sobre el RGPD (Murcia)

07/05/2018	Jornada en la CEOE sobre Protección de Datos
07/05/2018	Jornada Informativa para las PYMES sobre el RGPD (Canarias)
09/05/2018	Sesión sobre el RGPD en la Escuela de Organización Industrial
10/05/2018	Encuentro informativo sectorial sobre el RGPD "Publicidad"
16/05/2018	Jornada en la Cámara de Comercio de España para las PYMES sobre el RGPD
16/05/2018	Jornada Informativa para las PYMES sobre el RGPD (Zaragoza)
17/05/2018	Encuentro informativo sectorial sobre el RGPD "Gasista y Operadores de Productos Petrolíferos"
18/05/2018	Jornada Informativa para PYMES sobre el RGPD (Melilla)
21/05/2018	XII Foro Asociación Española de Profesionales de Turismo (AEPT), sobre el RGPD y el Proyecto de Ley Orgánica de Protección de Datos
28/05/2018	Taller sobre la Hoja de Ruta para la Adaptación al RGPD (Consejo General de Secretarios, Interventores y Tesoreros de la Administración Local)

08/06/2018	Foro Español de Laboralistas (FORELAB) Aspectos laborales del nuevo RGPD y su impacto en las relaciones laborales
20/09/2018	Jornada en el Colegio de Administradores de Fincas Colegio Oficial Ingenieros de Telecomunicaciones
21/09/2018	Taller para Delegados de Protección de Datos de la Administración General del Estado
25/09/2018	Curso RGPD – Comunidad de Madrid
02/10/2018	Foro RGPD para Ayuntamientos – Comunidad Rural Digital – (Salamanca)
04/10/2018	Taller para Delegados de Protección de Datos de las Administraciones Autonómicas
04/10/2018	Curso: "Nuevas obligaciones derivadas del Reglamento de protección de datos. transparencia y protección de datos en las entidades locales" Diputación de Palencia
17/10/2018	Jornada Protección de Datos de la Escuela de Administración Pública de Castilla y León (Valladolid)
11/12/2018	Taller para Delegados de Protección de Datos de Diputaciones Provinciales, Cabildos y Consejos Insulares

4. La potestad de supervisión (Inspección)

4.1 Adaptación a los cambios normativos

El año 2018 ha supuesto un punto de inflexión en la actividad de la Subdirección General de Inspección, especialmente, como consecuencia de la aplicación efectiva el 25 de mayo de 2018 del Reglamento General de Protección de Datos y de los novedosos modelos de cumplimiento y supervisión que incorpora.

Entre ellos reviste particular importancia la puesta en marcha de los mecanismos de cooperación y coherencia entre las autoridades de control de los Estados miembros.

En 2018 se han desarrollado y se han implantado los procedimientos colaborativos entre las autoridades de protección de datos de los Estados pertenecientes a la Unión Europea, para la gestión de incidencias que pueden incumbir a varios Estados.

Estos son los denominados procedimientos transfronterizos. Para gestionarlos, la Agencia ha debido incorporarse al sistema IMI (Internal Market Information System), que tienen que emplear las autoridades de control de los Estados miembros de la Unión Europea para comunicarse entre sí, según se describe posteriormente.

En los dos meses inmediatamente anteriores al 25 de mayo, así como en los meses que han seguido a esta fecha, la entrada de reclamaciones ha experimentado un importante incremento. Las causas pueden hallarse en las campañas de información que se han realizado sobre el Reglamento, y en la aparición de casos importantes y mediáticos en relación con el tratamiento de datos personales (Facebook-Cambridge Analytica, Google-Android, I-dental y otros) que han aumentado el grado de sensibilización de la opinión pública.

Además, en 2018 prosiguieron en las Cortes Generales los trámites para la aprobación del Proyecto de nueva Ley Orgánica de Protección de Datos Personales. A la vista de que su tramitación se extendería más allá de la fecha de plena eficacia del RGPD, fue preciso proponer una norma de transición, para dotar de cobertura a algunos aspectos relevantes, tales como la prescripción de infracciones y sanciones, las atribuciones de las actividades de investigación e inspección, o los trámites específicos en supuestos de tratamientos transfronterizos, entre otras cuestiones. Así, se aprobó el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.



Este proceso normativo culminó con la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Esta paulatina modificación de la normativa sobre el derecho fundamental a la protección de datos hizo que a lo largo de 2018 hayan convivido cuatro regímenes jurídicos distintos: el derivado de la Ley Orgánica 15/1999 (de aplicación a los expedientes iniciados antes del 25 de mayo de 2018), el establecido en el RGPD desde el 25 de mayo hasta el 31 de julio (fecha de la entrada en vigor del Real Decreto-ley 5/2018, de 27 de julio), el aplicable desde el 31 de julio hasta el 6 de diciembre, y el derivado de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en vigor desde el 7 de diciembre. Debido a esta situación el escenario de tramitación de procedimientos ha sido singularmente complejo.

Asimismo, cabe destacar entre las novedades de la Subdirección General de Inspección implantadas en 2018, la tramitación de expedientes propuestos desde la Unidad de Evaluación y Estudios Tecnológicos (UEET), a raíz del registro de notificaciones de brechas de seguridad.

A consecuencia de todo ello la Subdirección General de Inspección se ha reestructurado para adecuar su labor a este nuevo contexto.

4.2 La evolución de la subdirección general de inspección

Al objeto de incrementar la eficiencia de la Subdirección General, se ha modificado su composición interna. Antes constaba de un Área de Admisión y varias áreas temáticas, en las que se realizaban las actuaciones de investigación e inspección y se tramitaban los procedimientos sancionadores, en su caso, en función de la materia de la reclamación. Además, existía un Área de Seguimiento y Calidad.

Actualmente, la Subdirección está formada por el Área de Admisión, el Área de Traslados, el Área de Gestión de reclamaciones, el Área de Auditorías y el Área de Seguimiento y Calidad.

El Área de Admisión se encarga de realizar el primer análisis de los hechos y de la información disponible para determinar si se admitirá o inadmitirá el caso.

El Área de Admisión, en coordinación con el Área de Traslados, analiza el alcance territorial de la reclamación, para determinar si debe ser tramitada por la AEPD, o bien por otra autoridad de control de otro de los Estados de la Unión Europea. Esta decisión se adopta en función de varios criterios: en qué estado tiene la sede o establecimiento principal el responsable del tratamiento de datos objeto de la reclamación; en qué estado reside el afectado (o los afectados, o la mayor parte de ellos) y finalmente, ante qué autoridad de control se ha presentado la reclamación.

Si se considera que la reclamación tiene alcance transfronterizo, el Área de Traslados registra el caso en la plataforma IMI para que se determine cuál debe ser la autoridad líder, o bien, cuando se considera que la AEPD es la autoridad que debe liderar la tramitación, para que otras autoridades puedan manifestarse como interesadas. Asimismo, revisa los casos introducidos por otras autoridades de la UE,

para determinar si la AEPD en algún caso debe ser líder o autoridad interesada.

Los plazos de admisión a trámite y los plazos de tramitación quedan automáticamente suspendidos cuando debe recabarse información o consulta a un órgano de la UE o a otra autoridad de control de protección de datos de los Estados de la UE.

En caso de que deba ser tramitada por otro país, la reclamación se remite a la autoridad de control competente para que sea allí sea cursada conforme al trámite oportuno. En consecuencia, la presentada ante la AEPD se archiva, notificándose al interesado qué país se hará cargo de su reclamación.

IMI es la plataforma que emplean las autoridades de control en materia de protección de datos de la Unión Europea para el registro de reclamaciones y otras incidencias referentes al tratamiento de datos personales, utilizando el inglés como idioma común para la tramitación. Contempla distintos tipos de procesos para varios supuestos, tales como la comunicación de una incidencia para la identificación de cuál deba ser la autoridad que lidere la gestión del caso, la comunicación de una incidencia para que otras autoridades de control se manifiesten como interesadas en el caso, la comunicación de brechas de seguridad, la emisión de informes y observaciones, la solicitud de cooperación mutua, y otras.

La participación de la Autoridad Española en los distintos procedimientos que se tramitan a través de IMI es variada. La AEPD es la novena autoridad europea en cuanto a número de notificaciones enviadas totales, la tercera en cuanto a procedimientos del art. 56 del RGPD iniciados, y la duodécima en cuanto a expedientes liderados.

Si la reclamación no tiene carácter transfronterizo, el Área traslada la reclamación al responsable (a la atención del DPD, en caso de haber designado uno), requiriéndole que

responda al reclamante e informe a la AEPD, a fin de obtener una solución lo más rápida posible a la reclamación planteada por el ciudadano.

El Área instruye, también, los procedimientos sancionadores por infracción de la LOPDGDD y por la infracción de ciertos preceptos de Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. También se encarga de la gestión de los expedientes transfronterizos por vulneración del RGPD que lidera la AEPD.

Por su parte, el Área de Auditorías se ocupa de realizar investigaciones de amplio alcance sobre el cumplimiento de la normativa en sectores concretos de actividad y en ámbitos específicos de responsables o encargados de tratamientos. Esta área analiza aquellos casos en que se advierten indicios de que hay problemas relevantes en el tratamiento. También dirige los Planes de Investigación Sectorial de Oficio.

El Área de Seguimiento y Calidad presta soporte horizontal a las restantes áreas de la Subdirección en cuestiones de coordinación, personal y enlace con el Área de Informática, y diseña estrategias de normalización y simplificación de los procedimientos y realiza funciones de estadística.



4.3 La tramitación de reclamaciones en el Marco del RGPD

La aplicación efectiva del Reglamento ha generado un salto cuantitativo y cualitativo respecto de las reclamaciones presentadas ante la Agencia y los procedimientos para su tramitación.

El número de entradas ha crecido de 10.657 en 2017 a 14.146 en 2018, lo que supone un incremento del 33% de las reclamaciones. Este incremento no solo tiene un impacto por la magnitud, sino también por su complejidad como consecuencia de su tramitación en inglés a través de la plataforma IMI y de la obligación de investigar las brechas de seguridad remitidas por la UEET, que pudieran ser constitutivas de infracción.

El desglose de las entradas recibidas en 2018 es el siguiente:

- ▲ Reclamaciones presentadas ante la AEPD: 13.005
- ▲ Casos procedentes de otras autoridades de control europeas: 594
- ▲ Notificaciones de brechas de seguridad: 547

El detalle de la evolución trianual puede consultarse en la sección de inspección de datos recogida en el Anexo “La Agencia en cifras”.

En este marco, se describen a continuación los procedimientos de tramitación de las reclamaciones.

Tras el registro de entrada, la Subdirección General de Inspección de Datos asume la tramitación de las reclamaciones. En un primer momento, se analiza si la reclamación reúne los requisitos para ser admitida a trámite, o si por el contrario debe inadmitirse.

La AEPD inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones

de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción. En todo caso se informará al reclamante no solo de los fundamentos jurídicos de la inadmisión, sino también cuáles son los organismos y la regulación aplicable al caso planteado por el ciudadano.

Caso de que se considere que la reclamación debe ser admitida, también se valorará la posible relación de esta reclamación con otra u otras ya admitidas y en tramitación, así como se harán unas primeras pesquisas para determinar si se dan elementos que obliguen a trasladar la reclamación a otra u otras autoridades de control europeas.

Este primer análisis, previo a la decisión de admisión o no de la reclamación, concluirá con su traslado al responsable del tratamiento directamente o a través de su responsable, para que analicen la reclamación y respondan adecuadamente al reclamante debiendo, además, enviar una copia de esa respuesta a la Subdirección General de Inspección, a la que también habrá de explicar las razones que dieron lugar a la reclamación, así como las medidas adoptadas para que en el futuro no vuelva a ocurrir una anomalía de esas características.

El nuevo modelo de gestión considera que la reclamación es una fuente de información, tanto para las autoridades como para los propios responsables, que deben actuar en un doble plano. Por un lado y con carácter inmediato corrigiendo, cuando proceda, la situación origen de la reclamación, lo que deberá de hacerse del modo más rápido. Por otra parte, también se actuará analizando las causas que dieron lugar a esa reclamación para proceder a la adopción de las medidas necesarias para evitar que otras personas no sufran perjuicios similares originados por esas

mismas causas. Esa actuación correctora no solo de la reclamación sino de sus propios procesos, es una concreción del principio de responsabilidad activa. El seguimiento y, en su caso, la apertura de expedientes de investigación sancionadores dirigidos a corregir los procesos es una concreción del principio de supervisión permanente.

Se valora también si el Delegado de Protección de Datos designado por el responsable del tratamiento, o directamente el responsable del tratamiento, conocían la incidencia que ha originado la reclamación y si se habían pronunciado sobre ella. La Agencia puede trasladarles la reclamación, debiendo éstos responder al reclamante en el plazo de un mes y acreditar ante la Agencia cuál ha sido la respuesta dada, causas que originaron el problema e información adicional que se pueda precisar referente al caso.

A la vista del informe del responsable o su DPD, podrá archivar la reclamación si la incidencia ha sido atendida por el responsable, sin perjuicio de que la Agencia, aplicando los poderes de investigación y correctivos que ostenta, pueda llevar a cabo posteriores actuaciones relativas al tratamiento de datos referido en la reclamación.

Tras este primer análisis, comprensivo de varios elementos, que se ha descrito anteriormente, la AEPD notifica, en un plazo no superior a 3 meses, si la reclamación se admite a trámite o si se inadmite.

Si la reclamación se refiere única y exclusivamente a la falta de atención de los derechos regulados en los artículos 15 a 22 RGPD (derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos), el procedimiento que se desarrolle tendrá una duración máxima de 6 meses.

Si se estima que hay indicios de una vulneración de la normativa, y en caso de que se considere necesario, puede acordarse la iniciación de actuaciones de investigación, para determinar con mayor precisión los hechos, las causas y su repercusión, así como la identidad de los responsables. Estas actuaciones no podrán tener una duración superior a 12 meses. Las actuaciones pueden concluir con una resolución de archivo (en caso de que no se encontrasen pruebas de la comisión de una infracción atribuibles a un responsable), o con una resolución de acuerdo de inicio de un procedimiento sancionador.

Disponiendo de indicios racionales de la comisión de una infracción, se acordará iniciar un procedimiento sancionador. Este procedimiento se tramitará en un máximo de 9 meses. Si se constata la comisión de una infracción y su responsable, concluirá con una resolución en la que se determinará la imposición de alguna (o varias, simultáneamente) de las sanciones establecidas en el art. 58.2 RGPD (apercibimiento, multa, limitación temporal o definitiva del tratamiento, orden de suspensión de flujos de datos hacia un destinatario en un tercer país, orden de atender la solicitud de ejercicio del derecho de un interesado, entre otras).

Si además de la multa, se impusiera alguna otra sanción, el abono de la multa no implicaría el cierre del expediente, ya que también habrá de comprobarse la ejecución de la medida impuesta.

Por otra parte, y sin perjuicio de la realización de las actuaciones de investigación o de la tramitación de los procedimientos sancionadores que procedan, la AEPD podrá acordar si es necesario en cualquier momento medidas provisionales, tales como el bloqueo cautelar de los datos o la obligación inmediata de atender el derecho solicitado.

Como último dato a señalar en lo relativo a la tramitación y sus novedades, puede indicarse que la LOPDGDD contempla en su artículo 50 la publicación de las resoluciones de la AEPD en su página web, y para ello se anonimizan previamente los datos personales que contienen.

A consecuencia de estos cambios en las estructuras, en los procedimientos y en los métodos de trabajo, los indicadores que venían empleándose para analizar la gestión quedan descontextualizados, puesto que el escenario ha cambiado profundamente.

En 2018 se inicia una nueva etapa, con un nuevo enfoque y nuevos procesos. Es por ello que no puede seguirse un criterio de continuidad respecto a las cifras de años anteriores, sino que deben plantearse los datos disponibles como los iniciales de una nueva etapa.

El tratamiento de las reclamaciones ha sido sensiblemente diferente para las presentadas en la primera mitad del año y en la segunda. Como las reclamaciones tienen un tiempo no despreciable de tramitación, nos encontramos con un primer semestre de 2018 en el que tanto las reclamaciones recibidas (denuncias más reclamaciones de tutelas) como las resoluciones emitidas sí pueden compararse con el mismo periodo de ejercicios anteriores, pero con un segundo semestre en el que han convivido reclamaciones en curso tramitadas conforme a la normativa anterior junto con nuevas reclamaciones que se tramitan de acuerdo a procedimientos nuevos.

Entre el 1 de enero y el 24 de mayo, como notas a destacar, puede señalarse en la entrada un incremento importante en el número de denuncias y reclamaciones de tutela de derechos respecto a ejercicios anteriores.

En cuanto a las resoluciones, la plena aplicación del RGPD obligó a la Subdirección General de Inspección a adaptar sus estructuras dando lugar a un 10,9% menos de resoluciones de la potestad sancionadora, y manteniendo con un

mínimo incremento del 1,44% la resolución de procedimientos de tutela de derechos.

En el marco de esta preparación previa a la entrada del RGPD puede situarse también el sensible incremento de los recursos de reposición, que se sitúan en el 9,11%.

En la segunda mitad del año, aplicándose el RGPD para las reclamaciones nuevas, debe señalarse que, igual que sucedió en el semestre anterior, las reclamaciones han crecido hasta alcanzar el 28% de incremento anual.

Adicionalmente, la Agencia recibió en este semestre a través de IMI 594 reclamaciones de otras autoridades europeas sobre las que ha tenido que pronunciarse en la fase de Traslados.

Por último, la Subdirección General de Inspección ha tenido que realizar actuaciones previas de inspección sobre las 16 notificaciones de brechas de seguridad trasladadas por la UEET.

Las inadmisiones a trámite (IT) han aumentado levemente en valores absolutos respecto a los años anteriores, pero disminuyen en proporción al volumen de entradas recibidas. Está prevista la puesta en marcha de un buzón guiado de reclamaciones que vaya orientando al reclamante sobre los requisitos necesarios para formular su reclamación, con lo que para el futuro se espera que las inadmisiones vayan reduciéndose progresivamente.

En cuanto a los traslados, en los meses en que se lleva implantando este procedimiento se han podido resolver 1.890, y solo en 531 casos las reclamaciones siguen abiertas y es preciso pasar a actuaciones previas, expedientes de tutelas de derecho de olvido, o expedientes sancionadores directos. En los tres primeros meses un 42% de las entradas se ha resuelto, y además en 863 casos se ha resuelto solucionando la reclamación planteada por el reclamante.

En relación con las reclamaciones recibidas a través del IMI o por la sede o registro de la propia Agencia con elementos transfronterizos, de los 395 casos analizados, la Agencia ha solicitado implicarse como interesada en 237 casos, liderar 11, y archivar al no estar interesados otros 147 casos.

En 157 casos la reclamación había sido planteada por Cuerpos y Fuerzas de Seguridad sobre videovigilancia, resolviéndose con una carta advirtiendo al propietario sobre la normativa a cumplir. Por último, en esta fase de traslados se ha incluido la remisión de reclamaciones a la APDCAT y a la AVPD por ser de su competencia.

Respecto a la tramitación de los procedimientos de tutela de derechos se han producido importantes novedades. Tras un traslado al delegado o responsable de la entidad reclamada, se abren como expedientes de tutela las relativas al derecho al olvido (146 resueltas en el ejercicio) mientras que las demás se van tramitando progresivamente como el resto de las reclamaciones. Las resoluciones de tutela no relativas a derecho al olvido en el segundo semestre corresponden prácticamente a reclamaciones presentadas en el primer semestre del año. Esto explica parcialmente el drástico descenso en el número de resoluciones de tutela durante el segundo semestre. Por otra parte, el tratamiento unificado de las reclamaciones tras su recepción también ha hecho desaparecer las antiguas tutelas de derechos con resultado de inadmisión, que ahora se engloban dentro de las inadmisiones a trámite de reclamaciones.

Por su parte, la estadística del segundo semestre sobre procedimientos sancionadores queda muy distorsionada respecto a otros años. Se ha acelerado el fin procedimientos en curso, incrementando algunas cifras, pero también ha disminuido la apertura de procedimientos sancionadores nuevos, puesto que el traslado ha resuelto muchas reclamaciones. Será preciso esperar unos meses para valorar objetivamente este indicador.

En cuanto a la eficacia administrativa, los datos muestran una importante mejora que se ha traducido en un inequívoco descenso en los tiempos de tramitación y resolución, gracias a los traslados. Así se refleja con claridad en la tabla sobre reclamaciones resueltas y tiempos de tramitación que se recoge en la sección de eficacia administrativa recogida en el Anexo “La Agencia en cifras”. Puede decirse que con el nuevo modelo se resuelve más en las primeras etapas y menos en las últimas.

Contrariamente, el número de reclamaciones resueltas ha crecido de forma muy leve, pasando de 11.617 a 12.517 (que incluye las 531 brechas comunicadas y no investigadas).

Finalmente, cabría hacer una mención a los recursos humanos y a los cambios en curso para responder a este cambio de contexto. En diciembre de 2017 trabajaban en la Subdirección General de Inspección un total de 64 funcionarios repartidos en las diferentes áreas. En diciembre de 2018, ese número llegaba solo a 67 personas considerando las altas y bajas producidas en el ejercicio.

Como se ha indicado anteriormente, por imperativo del RGPD la LOPDGDD contempla las reclamaciones transfronterizas, que requieren de una tramitación conjunta y en inglés, e implican una actividad de gestión más diversa.

Por ello, si bien han aumentado levemente en los últimos años los medios humanos con que cuenta la Agencia para tramitar este volumen creciente de reclamaciones, será preciso adecuar la dotación de personal para responder adecuadamente a este nuevo escenario.

A continuación, se incluye un cuadro comparativo y un gráfico sobre la evolución de las reclamaciones y la del personal de la Agencia desde el año 2007 hasta la actualidad.

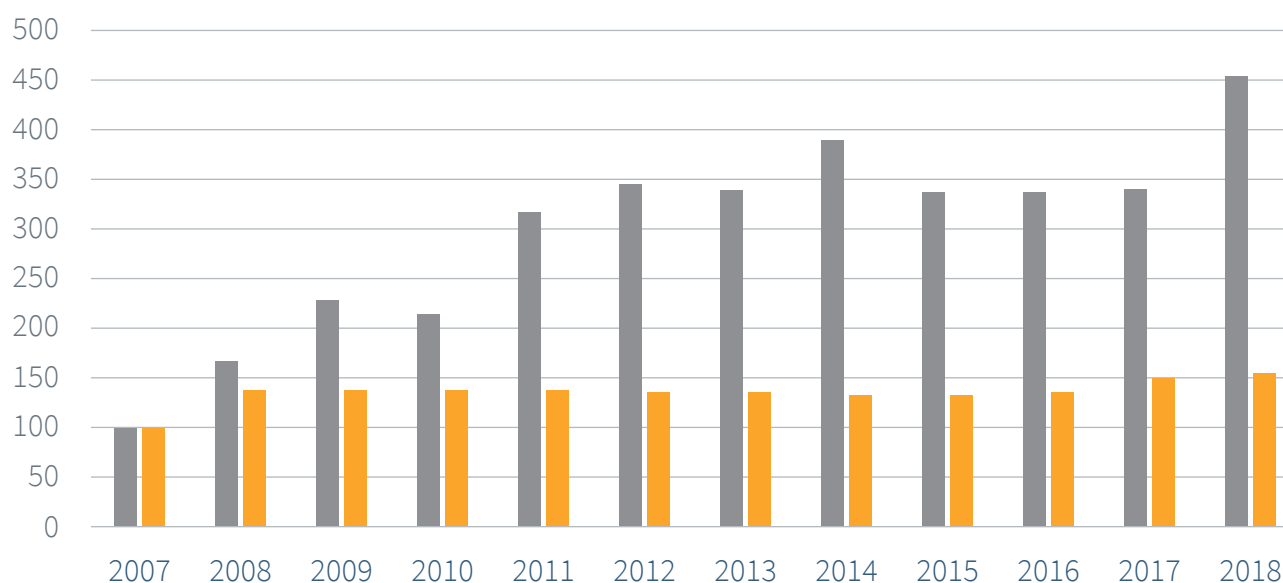
Evolución del número de reclamaciones y del personal de la AEPD

	Reclamaciones	Personal
2007	3.136	123
2008	5.232	167
2009	7.142	170
2010	6.702	168
2011	9.878	169
2012	10.787	165
2013	10.604	165

	Reclamaciones	Personal
2014	12.173	164
2015	10.571	164
2016	10.523	166
2017	10.651	181
2018	14.146	187
Δ 2007- 2018	351%	52%

Reclamaciones y Personal AEPD (base 2007)

■ Reclamaciones ■ Personal



4.4 Procedimientos más relevantes

4.4.1 Ámbito nacional

Entre los procedimientos más relevantes del ejercicio 2018 podemos destacar la resolución, en marzo de 2018, del expediente PS/00219/2017, en la que se declaran dos infracciones graves de la LOPD y se impone una sanción de 300.000 euros tanto a WhatsApp por comunicar datos a Facebook sin haber obtenido un consentimiento válido, como a Facebook por tratar esos datos para sus propios fines sin consentimiento.

La entidad WhatsApp fue adquirida por Facebook en el año 2014. En agosto de 2016, la primera actualizó los términos de su servicio y la política de privacidad, introduciendo cambios como el hecho de compartir información de los usuarios de WhatsApp con Facebook para finalidades que no tenían relación con la prestación del servicio de mensajería de dicha entidad.

La aceptación de esas nuevas condiciones se impuso como obligatoria para poder hacer uso de la aplicación de mensajería, tanto a los usuarios que ya tenían instalada la aplicación WhatsApp, como a los nuevos usuarios que pretendían instalarla.

La resolución analiza la información facilitada para la cesión de los datos concluyendo que se ofrece de forma poco clara, con expresiones imprecisas e inconcretas que no permiten deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos.

Así mismo, analiza las finalidades para las que se ceden los datos constatando, como se ha señalado, que no guardan relación con las finalidades que determinaron inicialmente su recogida y que no ofrece a los usuarios opción alguna para mostrar su negativa a la misma. La resolución concluye que la falta de precisión sobre los fines convierte en ineficaz

la información facilitada sobre los tratamientos de datos que se pretenden e impide al usuario conocer el uso al que se destinan sus datos personales. Por lo que no concurre el requisito de que se obtenga un consentimiento específico e informado.

En cuanto a la concurrencia del requisito de que el consentimiento no sea libre, la resolución no se limita a argumentar que la mera denegación del servicio si no se acepta la cesión de datos a Facebook determine su nulidad; sino que tiene en cuenta también otros aspectos, como son las consecuencias negativas de no poder hacer uso de la aplicación de mensajería WhatsApp, “considerando su implantación social”.

En relación con esta última cuestión, la resolución aunque se dicta en aplicación de la LOPD y de los criterios del Grupo del artículo 29 (Dictamen 15/2011) sobre la definición del consentimiento, señala que “para ayudar a entender esta conclusión, cabe citar” el Considerando 43 del RGPD en el que se afirma que el consentimiento no se puede considerar prestado libremente “cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando éste no sea necesario para dicho cumplimiento”. Aclarando que “con esta referencia no se pretende fundamentar la infracción conforme al nuevo Reglamento UE, (...), sino, simplemente, dejar constancia de la confirmación de aquel criterio en la nueva normativa, aplicable a partir del 25/05/2018”, según el criterio admitido por el Tribunal Supremo en su Sentencia de 13 de junio de 2016.

Otro procedimiento relevante al aplicarse por primera vez el RGPD, es el iniciado a la Liga Nacional de Fútbol Profesional (E/03318/2018) por publicar una app para dispositivos móviles

con capacidad de recoger sonidos de ambiente vulnerando la normativa de protección de datos. Esta investigación ha dado lugar a un expediente sancionador aun en curso.

El PS/00185/2018, se refiere a un instalador de una operadora telefónica que utilizó el teléfono móvil del cliente para proponerle una cita. Es, por tanto, un tratamiento sin consentimiento y desvió de finalidad. El caso salió en prensa como exponente de una mala práctica por parte de los instaladores.

En un expediente de investigación contra una entidad bancaria, los inspectores encontraron una hoja de cálculo con aproximadamente mil ochocientos registros de personas que se apuntaron a la bolsa de trabajo, incluyendo nombre, apellidos, teléfono, correo electrónico, y formación, lo que llevó a iniciar de oficio el PS/00116/2018, por presunta vulneración de las medidas de seguridad.

El procedimiento sancionador PS/00029/2018 provenía del incumplimiento de un apercibimiento. El reclamado manifestó que había tomado medidas, pero en realidad no dejó de hacer el tratamiento. Se trataba de un despacho de abogados que ganó un pleito relativo a una multipropiedad contra una inmobiliaria. El despacho de abogados conocía los datos de todos los clientes de la inmobiliaria, y empezó a enviarles publicidad por distintos medios. El caso es relevante por el número de usuarios afectados y porque se persistía en la conducta infractora, a pesar de haber sido objeto de un apercibimiento.

En el expediente A/00068/2018, se apercibe a un sindicato de médicos por enviar publicidad a los médicos de su comunidad autónoma lanzando propuestas contra el colegio de médicos. El caso se consideró de relevancia porque se señala que no todo lo que hace un sindicato se puede considerar actividad sindical.

En cuanto a casos relevantes contra administraciones públicas, puede citarse el

AP/00023/2018, contra el Ministerio de Trabajo, por ceder los datos a una ONG. Durante la instrucción del expediente de declaración de infracción, el Ministerio tomó la iniciativa y adoptó varias medidas, por lo que se declaró la infracción, pero no se requirieron medidas adicionales.

El expediente AP/00045/2018 se abrió de oficio tras la denuncia en diversos medios de la filtración de los resultados de un examen del MIR antes de su publicación oficial. En la resolución del expediente se declaró la infracción contra el Ministerio de Sanidad, pero se puso de manifiesto que ya se habían adoptado las medidas de seguridad apropiadas.

4.4.2 Ámbito transfronterizo

En cuanto a expedientes transfronterizos, vale la pena señalar varios casos abiertos por la Autoridad de Control española, que están siendo liderados por la Autoridad Irlandesa, y en los que nuestro país participa como autoridad interesada (art. 60 del RGPD). Es el caso del E/05055/2018 que se sigue contra Facebook por el consentimiento de su política de privacidad o el E/06584/2018 relativo a las cookies de esta red social. También destaca el E/00812/2019 contra la política de privacidad de OATH (antes AOL).

Pero la Autoridad de Control Española participa también como interesada en otros casos relevantes para nuestros ciudadanos como el que se sigue en Luxemburgo contra Amazon por procesamiento ilegal y cesión de datos a terceros, y los que se siguen en Irlanda contra LinkedIn, WhatsApp, Twitter e Instagram.

Por otra parte, España lidera 15 casos transfronterizos con el apoyo de otras autoridades interesadas y participa periódicamente en los grupos de trabajo internacionales para la mejora del sistema de intercambio de reclamaciones IMI y la homogenización de las multas.

4.5 Planes sectoriales o de auditoría

En el año 2018 ha continuado la ejecución de los planes en curso, y se han realizado otros adicionales como son los siguientes:

▲ Informe y Decálogo sobre “Políticas de privacidad en internet. Adaptación al Reglamento General de Protección de Datos”

El 17 de octubre de 2018 se publicó en el sitio web de la AEPD el informe sobre la adaptación de las políticas de privacidad online al Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), con el objeto de examinar el cumplimiento de la normativa por parte de las empresas y dictar recomendaciones a tal fin. La publicación del informe se acompañó de un decálogo con los aspectos más relevantes que deben tener en cuenta los responsables de tratamiento de datos personales para dar cumplimiento al RGPD.

Esta iniciativa, de carácter preventivo, se realizó para fomentar el cumplimiento de la legislación aplicable desde el 25 de mayo de 2018 y promover la sensibilización de las entidades que operan en Internet. Debido a la magnitud de la materia analizada, la Agencia seleccionó como muestra entidades de cuatro sectores (hoteles, transporte, comercio electrónico y seguros) y revisó empresas dedicadas a la venta de entradas online y a los servicios de música y contenidos de transmisión en tiempo real.

Hay que destacar que, desde el 17 de octubre de 2018, fecha en la que ambos documentos fueron publicados en la web de la AEPD, hasta finales del año 2018 se habían realizado un total de 6.090 descargas del decálogo y 9.310 del informe.

▲ Plan de Inspección Sectorial de Oficio de Entidades Financieras

El Plan de Oficio de Entidades Financieras tiene por objeto analizar la adecuación a la normativa vigente (RGPD y LO 3/2018) de protección de datos de determinados tratamientos realizados por el sector financiero y entidades conexas. Se viene desarrollando entre el segundo semestre de 2017 y se prevé finalizar al final del primer semestre de 2019.

Se debe señalar que las reclamaciones que recibe la Agencia relacionadas con el sector objeto de inspección suponen un tercio del total de las que se presentan anualmente.

Las organizaciones involucradas son las entidades financieras, pero también aquellas que dan soporte o participan en actividades de crédito. Además, se evidencia la expansión del mercado de los microcréditos, con plataformas que utilizan soportes digitales y mecanismos de autenticación a través de internet que presentan retos no sólo en la forma de identificar a los usuarios, sino en la forma en la que se tratan esos datos.

Hasta la fecha, en el marco de este plan de oficio se han realizado un total de 14 inspecciones presenciales a diversas entidades bancarias, financieras, de microcréditos y empresas tecnológicas que prestan servicios a las anteriores, además de 16 requerimientos de información.

Asimismo, se han completado las inspecciones presenciales y recibido la información requerida, estando a falta de elaborar el informe final del Plan Sectorial.

▲ Plan de Inspección sectorial de oficio de contratación a distancia

El plan sectorial de oficio sobre la contratación a distancia de productos y servicios tiene como objetivo analizar los procedimientos utilizados por las principales entidades que realizan la contratación de servicios o la venta de productos a través de las técnicas de venta telefónica y venta electrónica (Internet), detectar las debilidades de los procesos y proponer las mejoras necesarias a través de recomendaciones.

Su ejecución se realiza a lo largo de 2018 y finalizará el primer trimestre de 2019.

Durante 2018 se han completado las inspecciones presenciales a empresas de los sectores de venta de productos a través de la red, telecomunicaciones y comercializadores de energía eléctrica y gas, además de requerimientos de información mediante cuestionarios dirigidos a otras entidades. Durante 2019 se completarán el resto de las inspecciones programadas y se emitirá el informe del plan.

▲ Plan de inspección sectorial de oficio del sector sociosanitario

Este plan tiene como objetivo detectar los tratamientos y cesiones de datos que se llevan a cabo entre ambos sectores, social y sanitario y sus posibles vulnerabilidades, valorando su nivel de adecuación a la normativa de protección de datos, para así poder emitir recomendaciones que ayuden a elevar el nivel de cumplimiento del sector en esta materia.

Durante 2018 se ha hecho la investigación y el informe con los hallazgos y recomendaciones se emitirá en el primer semestre de 2018.

La primera y principal aportación de este plan ha sido evidenciar la inexistencia de un sector sociosanitario en España al carecer de una normativa reguladora, ni estructuras de

gobierno, documentos técnicos de consenso, programas asistenciales y recursos, como se desprende incluso del libro blanco de la coordinación sociosanitaria en España del Ministerio de Sanidad, Política Social e Igualdad.

Sí existe un sector social y un sector sanitario, siendo preferible hablar, más que de un sector sociosanitario, del denominado espacio sociosanitario, donde se coordinan los servicios sociales y los sanitarios para prestar una atención integral al usuario, con servicios transversales y multidisciplinares que atiendan a los individuos de forma más eficaz y de acuerdo a sus necesidades específicas.

Portanto, se ha intentado definir este espacio y acotar sus actores y relaciones, dado que es un espacio muy amplio y definido muy vagamente. El plan de investigación de 2018 se ha centrado en un subconjunto de dicho espacio que podrá extenderse a otros subconjuntos en futuros planes sectoriales.

▲ Evaluación Schengen de España. Plan SIS/ VIS del acervo Schengen

Las actividades desarrolladas en 2018, siguiendo un Plan de Auditoría continuo a cuatro años en estrecha colaboración con los responsables de los sistemas, han sido la realización de dos reuniones de seguimiento de la AEPD con la Oficina SIRENE, la Secretaría de Estado de Seguridad y el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, con el establecimiento de un calendario de inspecciones.

Además, se han realizado inspecciones presenciales a la Policía Foral de Navarra, se ha realizado un seguimiento al responsable SIS y se ha planificado la inspección a la Ertzaintza, todo ello en el seno del plan SIS.

Las actividades de supervisión sobre el sistema VIS, tras las ya ejecutadas en 2017, fueron la inspección al Consulado de España

en Shanghái, Quito y Londres y a la empresa subcontratada para la gestión del proceso de recogida de datos, BLS International Services LTD en cada uno de estos Consulados. Tales actuaciones dieron lugar en 2018 a la realización de informes parciales sobre su adecuación. Las recomendaciones serán incluidas en el informe final que se va a elaborar antes de mayo de 2019 y será remitido a los responsables para que realicen las alegaciones que consideren precisas. Estas alegaciones serán incluidas en el informe, estableciéndose un calendario de subsanaciones a las deficiencias detectadas.

El pasado 29 de noviembre se realizó la presentación del informe sobre la evaluación a España al Comité Schengen de la Comisión Europea, que aprobó el documento por consenso.

▲ Evaluación Schengen a otros países

Se ha participado en la Evaluación Schengen a Estonia en la parte de Protección de Datos en la semana del 16 al 21 de septiembre en Tallin.

El informe realizado en esa semana se recibió para comentarios el 23 de noviembre, que se aportaron el 26 de noviembre.

5. Una estructura en permanente evolución

5.1 Adaptación interna

Con el nuevo RGPD, la Agencia ha puesto en marcha nuevos procedimientos electrónicos para los ciudadanos, empresas y administraciones públicas en la Sede electrónica de la Agencia y siendo esta vía de comunicación obligatoria para las personas jurídicas.

Asimismo, ha sido necesario adaptar los formularios de inicio de trámites existentes a la nueva normativa.

- ▲ Nuevo formulario de solicitud de Consultas previas
- ▲ Nuevo formulario de notificación de Brechas de Seguridad
- ▲ Nuevo formulario de reclamaciones de derechos

La Agencia ha trabajado también en la generación de los flujos de tramitación necesarios para los nuevos procedimientos de gestión de notificaciones de brechas de seguridad y gestión de consultas previas en materia de protección de datos, que serán finalizados en la siguiente anualidad.



5.2 Sede y tramitación electrónica

Actualmente, más del 90 % de las comunicaciones con la Agencia continúan realizándose en formato electrónico, siendo la sede electrónica el canal prioritario con más del 70 % de las transacciones.

Desde 2017, los sistemas de información de la AEPD ya ofrecen las funcionalidades principales (sistema gestor de expedientes, Sede/Registro electrónico, Firma electrónica reconocida y Notificaciones electrónicas) que permiten realizar los trámites administrativos con medios electrónicos.

En 2018 se ha implantado la posibilidad de notificación electrónica a personas físicas para aquellos procedimientos que el usuario seleccione. Asimismo, se ha conseguido implantar una vía de comunicación con el Sistema de Intercambio de Registros de manera manual, quedando pendiente la interconexión automática para casos de envío masivo, principalmente desde el procedimiento de gestión de reclamaciones.

5.3 Puesto de trabajo digital

Buscando aumentar la productividad de sus empleados y siguiendo las directrices de la Estrategia Digital para la Administración General del Estado, la Agencia apuesta por desarrollar el puesto de trabajo digital, implantando herramientas de colaboración en la nube, que aseguran el contacto permanente con los equipos de trabajo y acceso a toda la información necesaria en cualquier momento y lugar. Esta solución dota a la Agencia de herramientas de uso general tales como sitios web de colaboración para compartir información de manera eficiente y segura dentro y fuera de la Agencia y acceso centralizado a recursos compartidos de manera ágil y ordenada. Además, esta solución se conforma como

habilitador de nuevas soluciones innovadoras proyectadas para los años siguientes tales como una nueva Intranet corporativa y un tramitador de propósito general que permita digitalizar pequeños trámites como la solicitud de teletrabajo o la coordinación de visitas institucionales.

5.4 Actualización continua

Una vez asegurados los objetivos derivados del nuevo Reglamento, la Agencia ha realizado un importante esfuerzo en actualización de los sistemas de información y de su infraestructura, del software de base y del modelo de provisión de servicios externalizados. Durante el segundo semestre, se han sacado al mercado los principales servicios y proyectos que verán la luz en los ejercicios 2019 y 2020.

5.5 Programa de teletrabajo

En el marco del proceso de modernización y de búsqueda de una mayor calidad del servicio público, la Agencia Española de Protección de Datos está decidida a atraer y retener a los mejores profesionales. En este entorno, el teletrabajo se presenta como una innovadora forma de prestación laboral que se está consolidando como una herramienta flexible, capaz de incrementar la productividad del tiempo de trabajo de los empleados públicos basándose en las múltiples prestaciones que ofrecen las tecnologías de la información y la telecomunicación.

Partiendo del compromiso de la Agencia Española de Protección de Datos con los citados principios de funcionamiento, con el objeto de mejorar la calidad de la prestación de los Servicios Públicos, tras una primera experiencia Piloto de Teletrabajo en 2017, en la que participó un número reducido de funcionarios, en 2018 se volvió a convocar, ya como programa habitual de trabajo, por Resolución de la Directora de la AEPD: durante 2018 han participado 46 funcionarios lo que supone que,

aproximadamente, un 30% de la plantilla de la AEPD ha teletrabajado dos jornadas semanales.

La participación se ha distribuido de forma bastante similar entre hombres y mujeres y por unidades y, dentro de los perfiles de los participantes, han predominado los que desempeñan puestos con un alto nivel de responsabilidad y autonomía a la hora de realizar su trabajo. La Secretaría General ha realizado el seguimiento del programa tanto en lo relativo al grado de satisfacción de los empleados públicos participantes, como en términos de rendimiento de las unidades.

El procedimiento seguido ha consistido en recabar información y opinión de todas las partes implicadas: participantes, supervisores y titulares de las subdirecciones mediante encuestas. Por resolución de 21 de noviembre de 2018, la dirección de la AEPD aprobó un nuevo programa, que será de aplicación en 2019.

5.6 Gestión presupuestaria y necesidades de Recursos Humanos y Materiales

La gestión presupuestaria en ejercicio, con un presupuesto prorrogado hasta el mes de julio y el aprobado posterior con un pequeño incremento del 0,9%, no ha supuesto grandes cambios con respecto a ejercicios anteriores, salvo en el nivel de ejecución, que ha sido superior 88,5% en 2018 frente a 82% en 2017, particularmente en el capítulo 1 debido al incremento de puestos de trabajo y, sobre todo, a la subida de retribuciones aprobada en la Ley General de Presupuestos del Estado para 2018, que supuso una mejora del 2,25%.

El Presupuesto 2018 se nutre como en años anteriores principalmente de 9.127.610 euros por sanciones y 5.051.270 euros de remanente de tesorería.

No obstante, en 2018 se han recibido aportaciones importantes por transferencias

de la Unión Europea por un importe total de 1.140.567,34 euros en lugar de los 20.000 euros con los que se contaba como compensación por reuniones del Comité Europeo de Protección de Datos y sus subgrupos de trabajo. Destacan, por su importe, los ingresos de fondos FEDER recibidos en los meses de noviembre y diciembre de 190.580,74 euros y 961.356,99 euros como compensación por las inversiones realizadas por la Agencia Española de Protección de Datos entre el 1 de enero de 2007 y 31 de diciembre de 2015 en Administración Electrónica.

Por otra parte, se han recibido ingresos por tres proyectos europeos en los que la Agencia participa:

- ▲ **Proyecto T4D4 (BASSO):** 58.196,17 euros para la formación de delegados de protección de datos en la Administración Local.
- ▲ **Proyecto SMOOTH:** 97.500 euros para el desarrollo de herramientas de ayuda al cumplimiento del Reglamento General de Protección de Datos de las pymes y micropymes europeas.
- ▲ **Proyecto PANELFIT:** 107.062 euros para uso ético de las Tecnologías de información y comunicación.

En materia de recursos humanos, los principales esfuerzos durante 2018 se han dedicado a mantener la cobertura del mayor número de puestos posible de la Relación de Puestos de Trabajo que a 31 de diciembre 2018 estaba dotada de 187 puestos, con unos índices de cobertura de en torno al 85%.

Para ellos se han publicado las correspondientes convocatorias de concursos de méritos y libres designaciones. A esta cifra de 187 puestos se ha llegado tras la recepción de algunos efectivos de Oferta de empleo Público y por la aprobación de un expediente de creación de 6 nuevos puestos en septiembre para reforzar las áreas más necesitadas de la AEPD: la unidad de Evaluación y Estudios Tecnológicos, la

Unidad de Apoyo de la Dirección, Informática en la Secretaría General, el Canal Informa y Subdirección General de la Inspección de Datos.

Una novedad importante de cara a 2019 que debe reseñarse es que la Ley Orgánica de Protección de Datos y garantía de los derechos digitales 3/2018, publicada el 6 de diciembre, habilita a la Agencia para elaborar y aprobar su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto.

Otra cuestión destacable en el ámbito de los Recursos Humanos ha sido el incremento de acciones formativas para el personal de la AEPD desarrolladas durante 2018 en diferentes ámbitos de conocimiento, entre otros, protección de datos, ofimática, auditoría de sistemas, promoción Interna a diferentes cuerpos de funcionarios de la Administración general del Estado, utilización del lenguaje administrativo o igualdad. Merece una mención especial el esfuerzo dedicado a la formación en el idioma inglés, que se ha convertido en idioma de trabajo para una parte de la plantilla; para ello, se han desarrollado clases durante todo el año y algunos talleres específicos para mejorar las capacidades de comunicación a través del correo electrónico o en las conversaciones telefónicas.

En materia de contratación, en 2018 toda la Administración ha debido realizar un importante esfuerzo de adaptación a la nueva Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. La entrada en vigor de esta ley en el mes de marzo ha hecho necesaria la adaptación de todos los pliegos de condiciones administrativas de los contratos y de la tramitación de los mismos, que ahora se realiza exclusivamente de forma electrónica a través de la plataforma de contratación del Sector público.

➤ 6. La necesaria cooperación institucional

6.1 Autoridades autonómicas

Con fecha 11 de julio tuvo lugar una reunión con la Agencia Vasca de Protección de Datos, para tratar asuntos de interés para ambas instituciones, en especial determinadas cuestiones en relación con el cumplimiento del Reglamento General de Protección de Datos. Asimismo, se han mantenido contactos con la Autoridad Catalana y la Agencia Vasca de Protección de Datos en relación con el seguimiento de la tramitación del proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

6.2 Relaciones con el Defensor del Pueblo

Se consolida durante este período la tendencia descendente marcada en el ejercicio anterior. En concreto, se han remitido a la Agencia desde la Oficina del Defensor del Pueblo un total de 17 asuntos, cuatro menos que en 2017.

Entre las principales materias o cuestiones que han sido objeto de la atención del Defensor del Pueblo, están las quejas relativas a la historia clínica (3) y a los llamados ficheros de morosos (2). Otras cuestiones que han sido objeto de queja han sido la oposición a las comunicaciones comerciales no solicitadas, o la difusión no autorizada de vídeos en las redes sociales.

Hay que destacar la queja formulada por el Defensor del Pueblo planteando la aparente contradicción entre la exigencia de una tasa autonómica para el acceso a una copia de la historia clínica y el principio de gratuidad que al respecto establece la normativa general de protección de datos, que ha dado lugar a la emisión de un informe del Gabinete Jurídico de la Agencia.

Asimismo, se recibió una queja en relación con un asunto que ha recibido en esta Agencia un gran número de reclamaciones (424 hasta el 16 de octubre), como es el relativo al cierre de las clínicas IDental, por no haber atendido el derecho de acceso a las historias clínicas de los afectados. Dicho asunto está siendo investigado por la Agencia, si bien ha tenido que ser objeto de suspensión debido a la apertura de diligencias judiciales por estos mismos hechos en la Audiencia Nacional.

Respecto a los principales motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, la mitad de ellos lo han sido para solicitar información sobre el estado de tramitación de su denuncia o recurso ante la falta de respuesta de la Agencia (8). Hay que señalar que en todos los casos la Agencia pudo justificar la notificación en plazo de las resoluciones mediante la correspondiente certificación acreditativa del servicio de correos.

Mediante los restantes escritos del Defensor del Pueblo se solicita a la AEPD que inicie actuaciones sobre los hechos objeto de queja, que profundice en su estudio, o bien que fije criterio en relación con algunos de los asuntos planteados.



6.3 Convenios

Además de los convenios y protocolos que se han citado en otros apartados de la memoria, la cooperación institucional de la Agencia se ha concretado en las siguientes iniciativas:

- ▲ Renovación expresa Convenio de colaboración CGPJ-AEPD-CENDOJ con objeto de articular la colaboración entre la Agencia Española de Protección de Datos y el Consejo General del Poder Judicial a través de su órgano técnico Centro de Documentación Judicial.
- ▲ Convenio entre la Universidad Internacional Menéndez Pelayo y la Agencia Española de Protección de Datos para la Organización de un Encuentro con objeto de regular la colaboración entre la UIMP y la AEPD para la organización conjunta del encuentro «El Reglamento General de Protección de Datos: orientaciones para su aplicación», del 2 al 4 de julio de 2018 en Santander en el marco general de los Cursos de Verano de la UIMP.
- ▲ Protocolo General de Colaboración entre la Agencia Española de Protección de Datos (AEPD) y el Consejo de Consumidores y Usuarios sobre actuaciones en relación con las prácticas irregulares en materia de contratación de servicios con objeto de establecer la colaboración entre el CCU y la AEPD en relación con la contratación irregular de servicios públicos.
- ▲ Protocolo General de Actuación entre la Comisión Nacional de los Mercados y la Competencia y la Agencia Española de Protección de Datos con objeto de establecer el marco general para el desarrollo de la colaboración entre la CNMC y la AEPD en los ámbitos especificados.

7. Una autoridad activa en el panorama internacional

7.1 Unión Europea

La entrada en aplicación del Reglamento General de Protección de Datos (RGPD) en mayo de 2018 supuso un cambio fundamental no solo en las normas que regulan los tratamientos de datos personales, sino también en la estructura institucional que en el ámbito europeo vela por la correcta aplicación del marco legal de la protección de datos.

En efecto, el RGPD establece el Comité Europeo de Protección de Datos (CEPD), que se configura como un organismo de la Unión, con personalidad jurídica propia, y con funciones que incluyen la de adoptar decisiones jurídicamente vinculantes para las autoridades de supervisión a fin de resolver los conflictos que puedan surgir entre ellas en determinadas actuaciones de aplicación del RGPD.

Son miembros del Comité los directores o presidentes de las autoridades de supervisión en materia de protección de datos de los Estados Miembro. Cuando en un Estado exista más de una autoridad, será designada una de ellas como representante común de las demás ante el Comité. En el caso español, es la Agencia Española de Protección de Datos la que asume esa representación común a las demás autoridades del Estado.

El Supervisor Europeo de Protección de Datos es también miembro del Comité, como lo son las autoridades de supervisión de los estados del Espacio Económico Europeo, aunque estas últimas, pese a su condición de miembros de pleno derecho, no tienen derecho a voto. La Comisión participa en las reuniones del Comité y debe ser informada de su actividad.

El Comité reemplaza al anterior Grupo Europeo de Autoridades de Protección de Datos (Grupo del artículo 29), pero las diferencias entre ambos son sustanciales.

Por un lado, y como ya se ha indicado, el CEPD es un organismo de la Unión y tiene personalidad jurídica propia. Esta nueva naturaleza tiene importantes consecuencias, entre las que pueden destacarse que está plenamente sometido a la normativa europea aplicable al funcionamiento de instituciones, agencias y organismos de la Unión, o el que sus decisiones vinculantes pueden ser objeto de recurso ante el Tribunal de Justicia de la Unión Europea.

Al mismo tiempo, sus funciones están sustancialmente reforzadas frente a las del Grupo del 29. Por una parte, y aparte de las ya repetidas decisiones vinculantes, el Comité puede adoptar también dictámenes que vinculan material, aunque no formalmente, a sus miembros. En caso de que una autoridad no siga uno de estos dictámenes, el incumplimiento será sometido a la consideración del Comité que podrá emitir una decisión vinculante en relación con el mismo.

Por otro lado, el Comité tiene la función de emitir recomendaciones, directrices o buenas prácticas en relación con una larga lista de materias. A pesar de que esos documentos no resultan jurídicamente vinculantes, la precisión con que se enumeran tanto esas materias como las acciones específicas que se asignan al Comité, junto con esa nueva naturaleza jurídica como organismo de la Unión, hacen que pueda afirmarse que el valor prescriptivo de todos esos documentos será aún mayor que el que ya tenían los dictámenes y recomendaciones del GT29.

El denominador común de todas estas funciones, tengan o no como resultado textos de carácter vinculante, es que persiguen dotar al Comité de los instrumentos para conseguir que actúe como el máximo órgano de coordinación y cooperación entre las autoridades de supervisión de la Unión a fin de garantizar conseguir una aplicación uniforme y coherente de la normativa de protección de datos.

La Agencia Española de Protección de Datos es consciente de la importancia del papel que el CEPD está llamado a desempeñar

Por ello se ha involucrado de forma muy activa en su funcionamiento. Esta implicación comenzó, incluso, antes del establecimiento del Comité. Por ejemplo, la AEPD formó parte del grupo de cuatro autoridades que redactaron las Reglas de Procedimiento del Comité.

Estas Reglas se diferencian de las que ya imperaban para el Grupo del 29 en el hecho de que deben regular unos procedimientos más complejos y con un mayor impacto tanto sobre los miembros del Comité como sobre terceros afectados por sus decisiones. Por ello, las Reglas han tenido que establecer procedimientos que aseguren la transparencia del proceso, la intervención de las partes afectadas y el respeto de sus derechos, así como el cumplimiento de los plazos previstos en el RGPD.

Aparte de ello, las Reglas regulan aspectos tales como la participación en las reuniones del Comité, su estructura de funcionamiento, los procedimientos de elección de presidente y vicepresidentes, la convocatoria y celebración de reuniones o, cuestión especialmente delicada en el ámbito europeo, el régimen

lingüístico de sus trabajos y de los documentos que el Comité produce.

Igualmente, la AEPD ha participado activamente en el diseño del Sistema de Información del CEPD. Este sistema sirve tanto como soporte para la actividad del Comité como para el intercambio de información entre las autoridades de supervisión en la aplicación de los mecanismos de cooperación y coherencia que prevé el RGPD.

El Sistema se ha desarrollado, siguiendo una decisión que adoptó el Grupo del artículo 29, a partir del sistema IMI. Se trata del sistema de información del Mercado Interior, del que son propietarios la Comisión Europea y los Estados Miembros y que se utiliza para el intercambio de información con objetivos vinculados al funcionamiento del Mercado Interior. La decisión del Grupo fue adoptada ante la imposibilidad de desarrollar “ex novo” un sistema de información que respondiera a las necesidades tanto del CEPD como de las autoridades nacionales.

El Sistema se implantó en el momento de establecimiento del Comité y ha funcionado con normalidad desde entonces, si bien se han producido varios ajustes de cierto calado para responder a algunas carencias y nuevas necesidades percibidas, y será reformado en breve para introducir nuevas funcionalidades. Dentro ya del marco de funcionamiento del Comité, es preciso hacer mención del que es el elemento central en la organización de sus trabajos: los subgrupos de expertos.

Estos subgrupos están integrados por representantes de las autoridades de supervisión y su principal misión es la de preparar las decisiones del Comité. Dicho en términos muy esquemáticos, prácticamente ningún documento o decisión es adoptado por el Comité sin que antes haya mediado el estudio y preparación de propuestas por parte de un subgrupo.

A finales de 2018 existían un total de 13 subgrupos de expertos, aunque algunos de ellos tienen un ámbito material de actuación muy restringido, como sucede con el “Subgrupo Multas”, cuya tarea es la identificar criterios comunes para la fijación de sanciones económicas en los Estados Miembro, o el “Subgrupo de Usuarios IT”, dedicado fundamentalmente a velar por el correcto funcionamiento y evolución del Sistema de Información del CEPD.

La AEPD participa en todos los subgrupos de expertos y es coordinadora de dos de esos subgrupos.

El primero de ellos es el denominado Subgrupo de Supervisión del Cumplimiento (“enforcement”), en el que actúa como coordinador junto con la autoridad holandesa. Este grupo tiene como misión la de actuar como foro de intercambio de información, coordinación y preparación de decisiones en materia de actuaciones llevadas a cabo por las autoridades nacionales en el ámbito de la inspección y sanción de infracciones.

Como ejemplo del modo en que se concreta esa misión, puede indicarse que para el año 2019 el subgrupo incluye en su programa de trabajo finalizar el desarrollo de una estrategia de “enforcement” para el CEPD; preparar un manual de comunicación en materia de inspección y sanción de infracciones; analizar los problemas asociados con la inspección y sanción de responsables no establecidos en la Unión Europea pero a los que se aplica el RGPD, identificando posibles soluciones; y establecer “grupos de contacto” para el seguimiento de procedimientos desarrollados en varios Estados Miembro en relación con una misma organización o con un mismo tipo de infracción al RGPD.

El segundo subgrupo de expertos en el que la AEPD actúa como coordinador es el denominado “Cumplimiento, Salud y Gobierno Electrónico”. Este subgrupo, cuyo ámbito material es, sin

duda, heterogéneo, es el resultante de integrar en un solo foro, que originariamente se dedicaba tan solo a cuestiones de gobierno electrónico, materias de relevancia para el Comité pero que no encontraban acomodo en otros subgrupos.

El programa de trabajo de este subgrupo para el año 2019 incluye, entre otras cuestiones, finalizar la adopción de unas directrices del Comité sobre códigos de conducta en el marco del RGPD; preparar la respuesta a varias consultas formuladas por la Comisión al CEPD en materias como ensayos clínicos o la relación entre el Reglamento de libre circulación de datos no personales en la UE y el RGPD; preparar los dictámenes del CEPD en relación con las cláusulas estándar de encargo de tratamiento que deseen adoptar las autoridades nacionales de supervisión y preparar un los dictámenes del Comité sobre las propuestas de criterios de acreditación de los organismos de supervisión de códigos de conducta propuestos por las autoridades nacionales.

El papel del coordinador es clave para el funcionamiento del subgrupo y para sus resultados. El coordinador preside las reuniones de los subgrupos, actúa como punto de contacto de los miembros del subgrupo, prepara el orden del día de las reuniones, distribuye los documentos, vela por que el desarrollo de las reuniones se adecúe a lo establecido en las Reglas de Procedimiento y reporta al Plenario del Comité sobre la actividad del subgrupo.

Parte importante de su papel consiste, también, en que los coordinadores de todos los subgrupos forman parte, a su vez, de otro subgrupo, el de “Coordinadores”, una de cuyas principales tareas es la de establecer los programas de trabajo de los diferentes subgrupos para cada año.

Las modificaciones en el marco normativo de la protección de datos en la Unión Europea han afectado también a otro ámbito material que, aunque relacionado con la actividad de la Unión, se había abordado hasta fechas recientes

desde la perspectiva de la cooperación entre los Estados Miembro. Se trata de la supervisión de la aplicación de la normativa de protección de datos en materia de cooperación policial y judicial penal.

En la Unión Europea se han desarrollado históricamente agencias o grandes sistemas de información orientados a promover y facilitar la cooperación entre los Estados Miembro en materia policial y judicial. Entre las agencias puede mencionarse Europol y entre los grandes sistemas el Sistema de Información Schengen o el Sistema VIS.

Esas agencias o grandes sistemas integran intercambios de datos personales entre las autoridades nacionales participantes, usando una infraestructura europea, o de esas autoridades entre sí y con una instancia central europea, que es el caso de las agencias europeas.

La supervisión de esos intercambios desde la perspectiva de la protección de datos se ha realizado a partir de un modelo tradicional, el de las “autoridades conjuntas de control”, que ha ido evolucionando paulatinamente a la figura de los “grupos de supervisión coordinada”. Estos grupos, que son los que actualmente están implantados en la mayoría de agencias o grandes sistemas de información, se basan en una supervisión coordinada sobre los diferentes niveles de utilización de los datos.

En el marco de sus competencias específicas, las autoridades nacionales se ocupan de los tratamientos a nivel nacional, mientras que el Supervisor Europeo de Protección de Datos hace un seguimiento de la actividad del sistema de información como tal o de la agencia europea afectada. Los grupos de coordinación sirven para asegurar la cooperación y la coherencia de la supervisión en esos diferentes niveles.

Hasta el año 2018 han existido una pluralidad de autoridades comunes de control o grupos de coordinación, con denominaciones diversas

y también con funciones diferenciadas, reguladas por los instrumentos de creación de las correspondientes agencias o sistemas. Así, junto con los ya mencionados pueden citarse Eurojust, Eurodac, o Aduanas.

Sin embargo, en 2018 se aprobó el Reglamento 2018/1725, que es el que regula la protección de datos en el ámbito de las instituciones, agencias y organismos de la Unión, reemplazando al anterior Reglamento 45/2001.

En este nuevo Reglamento se reitera el modelo de “grupos de coordinación”, en la medida que se prevé que el Supervisor y las autoridades nacionales ejercerán las labores de supervisión actuando cada uno en el marco de sus respectivas responsabilidades y competencias, debiendo intercambiar información y cooperar entre sí.

La diferencia, no obstante, estriba en que el Reglamento se aleja de la pluralidad de instancias de coordinación existentes para establecer que esa cooperación y coordinación deberá realizarse en el marco del Comité Europeo de Protección de Datos, donde el Supervisor y las autoridades nacionales deberán reunirse, al menos, dos veces al año.

Tras la aprobación del Reglamento 2018/1725, el Comité ha iniciado los trabajos para desarrollar las estructuras y métodos de trabajo adecuados para dar cabida a esta nueva función

Por el momento, la principal dificultad de esta tarea radica en la ya citada diversidad de tareas y funciones asumidos por las anteriores instancias de coordinación, que derivan de las previsiones que contienen las normas que regulan cada

agencia o gran sistema de información. En tanto no se modifiquen esas normas, el Comité deberá respetar esa diversidad de funciones.

La AEPD ha participado, y sigue haciéndolo, en todas las autoridades comunes de control y grupos de coordinación existentes. Está previsto mantener ese nivel de participación en el esquema de coordinación de la supervisión que se establezca en el marco del Comité Europeo.

7.2 La cooperación con Iberoamérica. Especial Referencia a la red Iberoamericana de Protección de Datos (RIPD)

Las principales actividades desarrolladas por la AEPD en relación con Iberoamérica, especialmente a través de la Red Iberoamericana de Protección de Datos (RIPD), en su condición de Secretaría Permanente, han sido las siguientes:

▲ Visitas a la AEPD de delegaciones de instituciones y parlamentarios chilenos

Para analizar diversos aspectos relacionados con el Proyecto de Ley chileno de protección de datos personales.

▲ Visita a la AEPD de delegaciones del Instituto de Transparencia

Acceso a la Información Pública y Protección de Datos del Estado de México (INFOEM), el Comisionado Presidente del INAI y la Superintendencia de Industria y Comercio de Colombia.

▲ Comité Ejecutivo de la RIPD

Con fechas 16 de abril y 9 de octubre, se celebraron sendas reuniones online del Comité Ejecutivo de la RIPD, en las que se debatieron, entre otras cuestiones, las relativas al XVI Encuentro Iberoamericano de Protección de Datos; la programación de las acciones

formativas para empleados latinoamericanos, en colaboración con la AECID y la Fundación CEDDET; la modificación del Reglamento RIPD para la participación de la delegación de la RIPD en las actividades de la Conferencia Internacional de Autoridades de Protección de Datos y de Privacidad a celebrar el próximo mes de octubre en Bruselas, y la admisión de nuevos integrantes de la RIPD, en su condición de observadores.

▲ VI Foro de Transparencia y Buen Gobierno

Por invitación de la Fundación Chile-España, asistió al citado Foro en representación de la Agencia el Coordinador de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia, quién participó como ponente en la Mesa Redonda “Transparencia y Protección de datos: cómo conciliar ambos valores”. La totalidad de los gastos fueron asumidos por el organizador.

▲ Participación de la RIPD en la 40ª Conferencia Internacional de Autoridades de Privacidad y Protección de Datos

El día 22 de octubre, en el marco de la Sesión Cerrada de la 40ª Conferencia Internacional de Autoridades de Privacidad y Protección de Datos se reservó un punto del orden del día para que la RIPD, a través de su Presidencia, la Unidad Reguladora y de Control de Datos Personales de Uruguay, presentase formalmente a la Conferencia los Estándares Iberoamericanos de Protección de Datos.

Por otra parte, el 23 de octubre, dentro de la programación paralela de la Conferencia, se reservó por primera vez un espacio propio para hablar del estado de la protección de datos en Iberoamérica, bajo la organización de la Red Iberoamericana de Protección de Datos, la Comisión Europea y el Supervisor Europeo de Protección de Datos. Por parte de la AEPD, y en representación de la Secretaría Permanente de la RIPD, intervino el jefe del Área Internacional de la AEPD, quien destacó la trayectoria y el

papel crucial que ha desempeñado la RIPD en el desarrollo del derecho fundamental en Iberoamérica a lo largo de sus quince años de existencia.

▲ Intervención del Presidente de la RIPD en el acto conmemorativo del 25 aniversario de la AEPD

El 13 de noviembre tuvo lugar en el Senado la intervención del Presidente de la Red Iberoamericana de Protección de Datos, Felipe Rotondo, en el marco de los actos del 25 aniversario de la AEPD, con una conferencia acerca de la labor de defensa de este derecho fundamental en el espacio iberoamericano.

▲ Participación de la AEPD en el XVI Encuentro Iberoamericano de Protección de Datos

La AEPD participó, del 28 al 30 de noviembre, en el XVI Encuentro Iberoamericano de Protección de Datos, que se celebró en San José de Costa Rica, bajo la organización de la Red Iberoamericana de Protección de Datos (RIPD) y la Agencia de Protección de Datos de los Habitantes de Costa Rica (PRODHAB).

El Encuentro reúne anualmente a los Miembros, observadores y expertos que integran la RIPD, así como a representantes de los sectores privados y empresariales, la Universidad, expertos y profesionales de la privacidad de Iberoamérica, Estados Unidos, Canadá y Europa. En su Sesión Abierta, los días 28 y 29 de noviembre, se abordaron temas como los nuevos procesos de adecuación; las relaciones entre las autoridades de control y los sujetos obligados; la protección de los datos personales de los menores; el papel de las redes, las organizaciones sociales y las asociaciones profesionales; la inteligencia artificial, así como el blockchain y la privacidad desde el diseño, entre otros.

La representación de la AEPD intervino como Ponente en los Paneles que llevaban por título ‘Las relaciones entre Autoridades y

sujetos regulados. Nuevas estrategias’, ‘Nuevas perspectivas para los tratamientos de datos en la investigación sanitaria’ y ‘Los otros actores de la protección de datos. El papel de las redes, las organizaciones sociales y los profesionales de la privacidad’.

La Sesión Abierta contó con una amplia asistencia de cerca de 300 participantes de los ámbitos profesional, académico y del sector público. El evento fue clausurado por la Directora de la AEPD, como Secretaria Permanente de la RIPD, el Encargado Comercial de la Embajada de la UE, la Ministra de Justicia y Paz, la Directora de la PROHAB y el Presidente de la República, quien manifestó el firme compromiso de su país con la protección de los datos personales, anunciando la próxima adhesión de Costa Rica al Convenio 108 del Consejo de Europa.

En la Sesión Cerrada se debatieron diversas cuestiones que afectan a la organización y funcionamiento interno de la Red, siendo los acuerdos más destacados: la aprobación de la revisión del Reglamento interno de la RIPD, fundamentalmente para incorporar a las organizaciones sociales; la renovación por otros dos años en la Presidencia de la Red de la URCDP de Uruguay, así como del Comité Ejecutivo actual.

▲ Plan de formación de empleados de agencias y otras entidades públicas latinoamericanas

En el marco del programa Interconecta de la AECID, en colaboración con la Fundación CEDDET, y bajo la dirección y con profesorado de la AEPD, se ha puesto en marcha este año la primera edición de un itinerario formativo sobre el Reglamento General de Protección de Datos, con dos ciclos o etapas: una etapa inicial (Curso de Experto RIPD en PDP), y un segundo ciclo (Curso de Especialista RIPD en PDP).

▶ ANEXO

LA AGENCIA EN CIFRAS

1. Actividad global

Resumen de actividad global

El desglose de estas y otras actividades se detalla en páginas posteriores de esta sección.

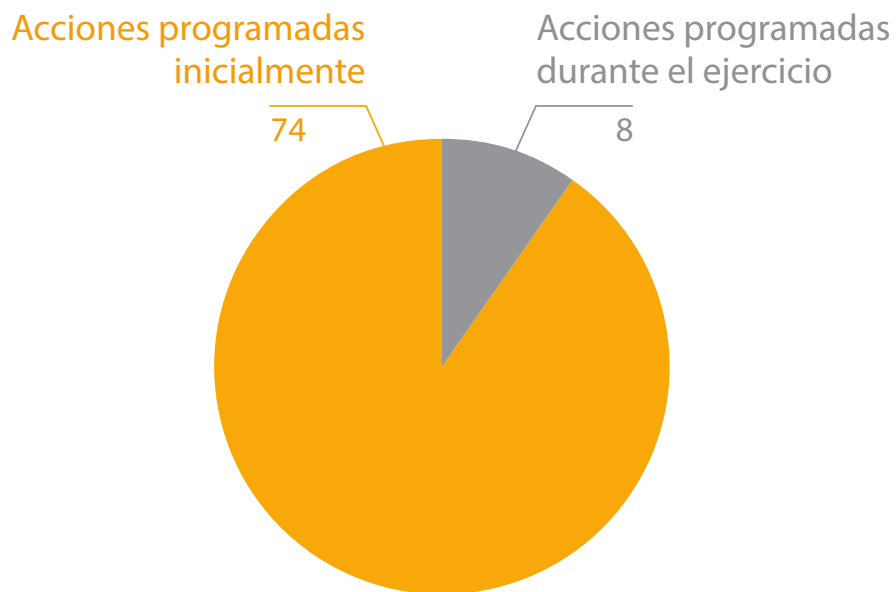
Resumen de actividad global			
	2017	2018	Δ% 2017-2018
Actuaciones del Plan Estratégico ejecutadas o puestas en marcha	78	79	1,28%
Entradas recibidas (reclamaciones planteadas + notificaciones de quiebras de seguridad)	10.657	14.146	32,74%
Entradas resueltas (reclamaciones + notificaciones quiebras de seguridad)	11.617	12.517	7,75%
Consultas atendidas Atención al ciudadano	255.908	749.020	192,69%
Consultas atendidas INFORMA_RGPD**	-	4.116	-
Visitas recibidas en la web	6.724.113	7.925.300	17,86%
Consultas especializadas sobre tratamiento de datos de menores	895	1.564	74,75%
Delegados de Protección de Datos notificados*	-	20.043	-
Cuestionarios finalizados con la herramienta Facilita_RGPD	6.196	150.360	2.326,73%

*La comunicación de Delegados de Protección de Datos es obligatoria desde el 25 de mayo de 2018.

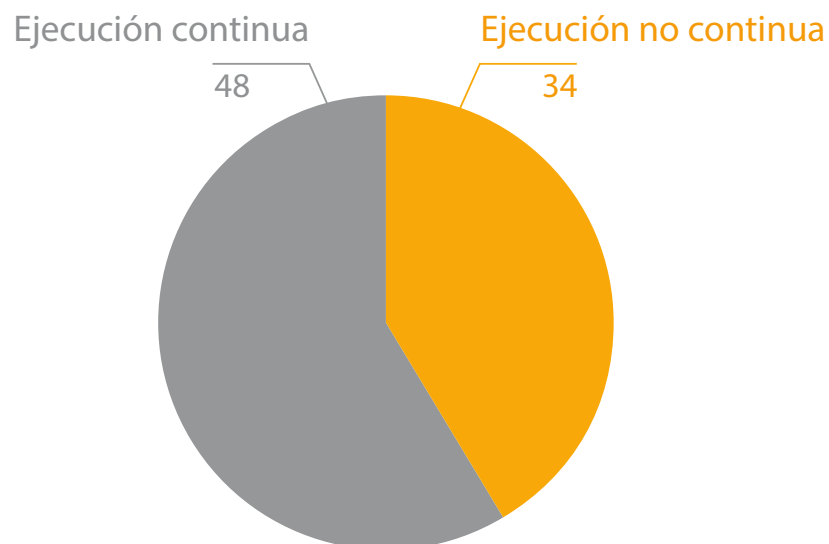
**Canal disponible desde marzo de 2018.

2. Plan estratégico

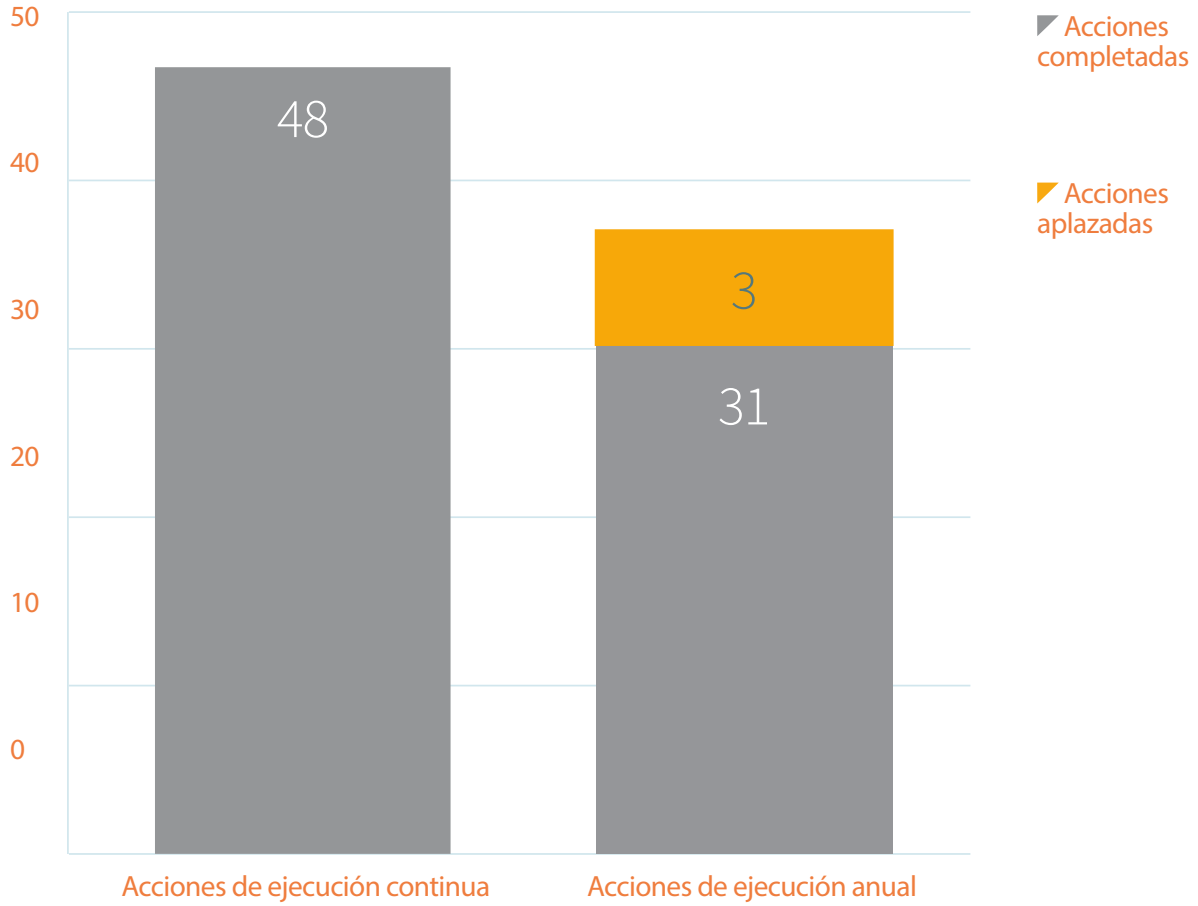
Acciones programadas en 2018



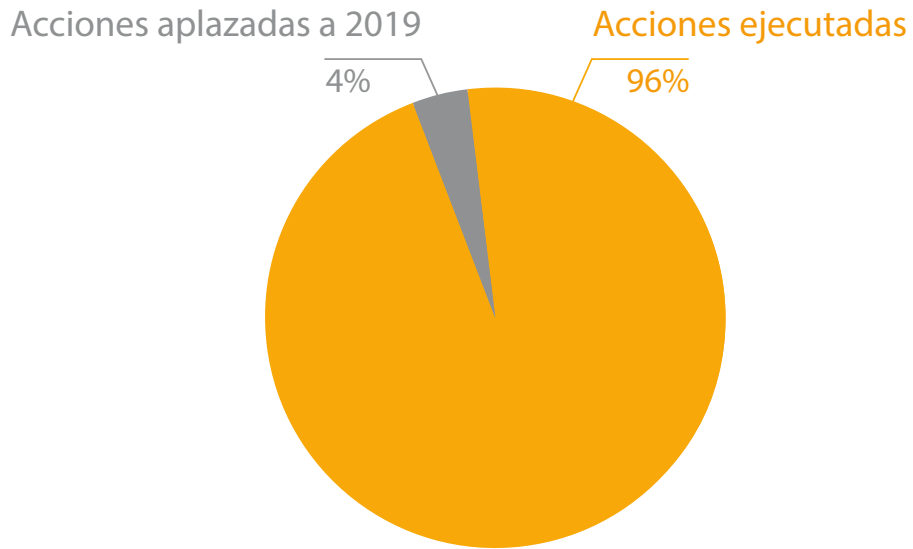
Tipo de ejecución



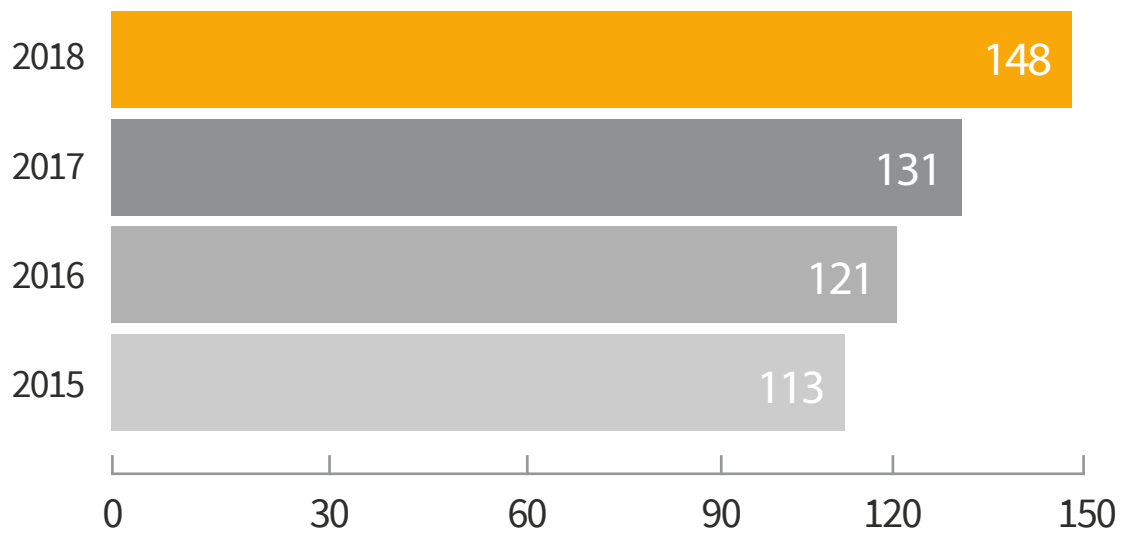
Grado de ejecución



En porcentaje



Evolución iniciativas del Plan - Periodo 2015-2018



3. Inspección de datos

Datos globales

A partir del 25 de mayo de 2018 las denuncias y las reclamaciones de tutela pasan a denominarse reclamaciones siguiendo la nomenclatura del Reglamento General de Protección de Datos.

Entradas recibidas durante el ejercicio

El art. 33 del RGPD desarrolla la obligación de notificar las violaciones de seguridad a la Autoridad de Control. Durante el segundo semestre de 2018 el número de notificaciones de brechas de seguridad registradas ha sido muy significativo. Estas notificaciones son registradas por la Unidad de Evaluación y Estudios Tecnológicos (UEET), que tras un primer análisis determina si deben ser origen de un expediente de investigación conducido por la Subdirección de Inspección o no. Bajo el epígrafe genérico de entradas recibidas se incluyen dos tablas separadas para reclamaciones y notificaciones de brechas de seguridad.

	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Reclamaciones presentadas en la AEPD	-	-	13.005	96%	-	-
Casos procedentes de otras AC europeas	-	-	594	4%	-	-
Reclamaciones de tutela	2.588	2.654	-	-	-	-
Denuncias	7.935	7.997	-	-	-	-
TOTAL RECLAMACIONES	10.523	10.651	13.599	100,00%	28%	29%
Notificaciones de brechas de seguridad registradas	1	6	547	-	9017%	54600%
TOTAL NOTIFICACIONES DE BRECHAS DE SEGURIDAD	1	6	547	-	9017%	54600%
Total Reclamaciones	10.523	10.651	13.599	96,13%	28%	29%
Total Notificaciones brechas seguridad	1	6	547	3,87%	9017%	54600%
TOTAL ENTRADAS RECIBIDAS (RECLAMACIONES + BRECHAS DE SEGURIDAD)	10.524	10.657	14.146	-	33%	34%

Entradas resueltas durante el ejercicio

En un primer análisis realizado por la UEET se decide cuáles de las notificaciones de brechas recibidas requieren un expediente de investigación, y cuáles no. En los años anteriores a 2018 el número de notificaciones de brechas de seguridad recibido era muy bajo, la propia Subdirección de Inspección se ocupaba de su registro, y todas ellas eran objeto de expedientes de investigación.

	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Reclamaciones resueltas en la AEPD	-	-	11.839	99%	-	-
Traslados. Reclamaciones resueltas por ser plena competencia de otras AC europeas	-	-	147	1%	-	-
Reclamaciones de tutela	2.471	2.824	-	-	-	-
Denuncias	8.112	8.793	-	-	-	-
TOTAL RECLAMACIONES	10.583	11.617	11.986	100,00%	3%	13%

	2016	2017	2018
Notificaciones de brechas de seguridad analizadas	-	-	531
TOTAL NOTIFICACIONES BRECHAS DE SEGURIDAD	-	-	531

	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
% respecto a las que han tenido entrada y pendientes del ejercicio anterior	78%	85%	77%	-	-8%	-1%
Total Reclamaciones	10.583	11.617	11.986	96%	3%	13%
Total Notificaciones de Brechas de seguridad analizadas	-	-	531	4%	-	-
TOTAL ENTRADAS RESUELTAS (RECLAMACIONES + NOT. DE BRECHAS)	10.583	11.617	12.517	100,00%	8%	18%

► Resoluciones

El número de reclamaciones tramitadas no tiene que coincidir necesariamente con las resoluciones firmadas: varias reclamaciones referidas a un mismo reclamado pueden agruparse, y paralelamente en una reclamación pueden aparecer múltiples reclamados dando origen a múltiples procedimientos.

Resoluciones según el tipo de procedimiento						
	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Archivo de actuaciones tras no subsanarse denuncia (hasta el 25 de mayo)	949	1.159	472	12%	-	-
*Traslado a delegado, responsable, videovigilancia u otras autoridades	18	65	1.956	49%	-	-
Archivo de actuaciones de investigación	883	907	658	16%	-27%	-25%
**Resolución de procedimientos de apercibimiento (hasta el 25 de mayo)	492	490	377	9%	-	-
Resolución de procedimientos sancionadores	573	731	434	11%	-	-
**Resolución de procedimientos de infracción de las AAPP (hasta el 25 de mayo)	56	60	96	2%	-	-
TOTAL	2.971	3.412	3.993	100%	17%	34%

*El procedimiento de los traslados al delegado o al responsable, como fase previa a la admisión de una reclamación se introdujo a partir de la publicación del RD 5/2018 el 30 de julio. A partir del 25 de mayo de 2018 comienza también a emplearse el mecanismo de ventanilla única entre las AC europeas.

**A partir del 25 de mayo de 2018 tanto los procedimientos de apercibimiento como los procedimientos de infracción de las AAPP pasan a engrosar el apartado de los procedimientos sancionadores, por lo que no pueden compararse los datos de 2018 en estos apartados (cinco primeros meses) con los ejercicios anteriores completos.

Resoluciones según sentido de la resolución						
	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Archivo de actuaciones tras no subsanarse denuncia (hasta el 25 de mayo)	949	1.159	472	12%	-59%	-50%
Traslados. Reclamaciones resueltas tras traslado al responsable y respuesta satisfactoria	-	-	863	22%	-	-
Traslados. Reclamaciones resueltas tras traslado de videovigilancia por denuncias FCSE	-	-	157	4%	-	-
Traslados. Reclamaciones resueltas por Acuerdos de remisión a AC autonómica	18	65	21	1%	-68%	17%
Traslados. Reclamaciones resueltas por ser plena competencia de otras AC europeas	-	-	147	4%	-	-
*Traslado a otra AC europea participando como AC interesada	-	-	237	6%	-	-
*Traslado. Reclamación no resuelta y admisión a trámite	-	-	531	13%	-	-
Archivo de actuaciones de investigación	883	907	658	16%	-27%	-25%
Archivo de procedimiento de apercibimiento (hasta el 25 de mayo)	311	289	227	6%	-	-
Archivo de procedimiento sancionador	100	119	65	2%	-	-
Archivo de procedimiento de infracción de las AAPP (hasta el 25 de mayo)	13	15	11	0%	-	-
Total resoluciones declarativas de infracción	697	858	604	15%	-30%	-13%
Declarativa de infracción con apercibimiento (hasta el 25 de mayo)	181	201	150	4%	-	-
Declarativa de infracción con sanción económica	473	611	369	9%	-	-
Declarativa de infracción de las AAPP (hasta el 25 de mayo)	43	46	85	2%	-	-
Total resoluciones de archivo	2.274	2.554	3.389	85%	33%	49%
TOTAL RESOLUCIONES POTESTAD SANCIONADORA	2.971	3.412	3.993	100%	17%	34%

*No ponen fin al procedimiento

Resumen de resoluciones emitidas

	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Resoluciones de la potestad sancionadora	2970	3409	3993	34%	17%	34%
**Resolución de procedimientos de tutela de derechos	2471	2818	927	8%	-	-
***No admisiones a trámite	6219	6368	6721	58%	6%	8%
*Total resoluciones que ponen fin a procedimientos	11.660	12.595	10.873	93%	-14%	-7%
TOTAL	11.660	12.595	11.641	100%	-8%	0%

*Excluye las resoluciones de traslado con Reclamación no resuelta y admisión a trámite, y los traslados a otra AC europea participando como AC interesada.

**En el 2018 las reclamaciones de tutela de derecho con resultado de inadmisión pasan a tratarse de forma conjunta con las inadmisiones a trámite

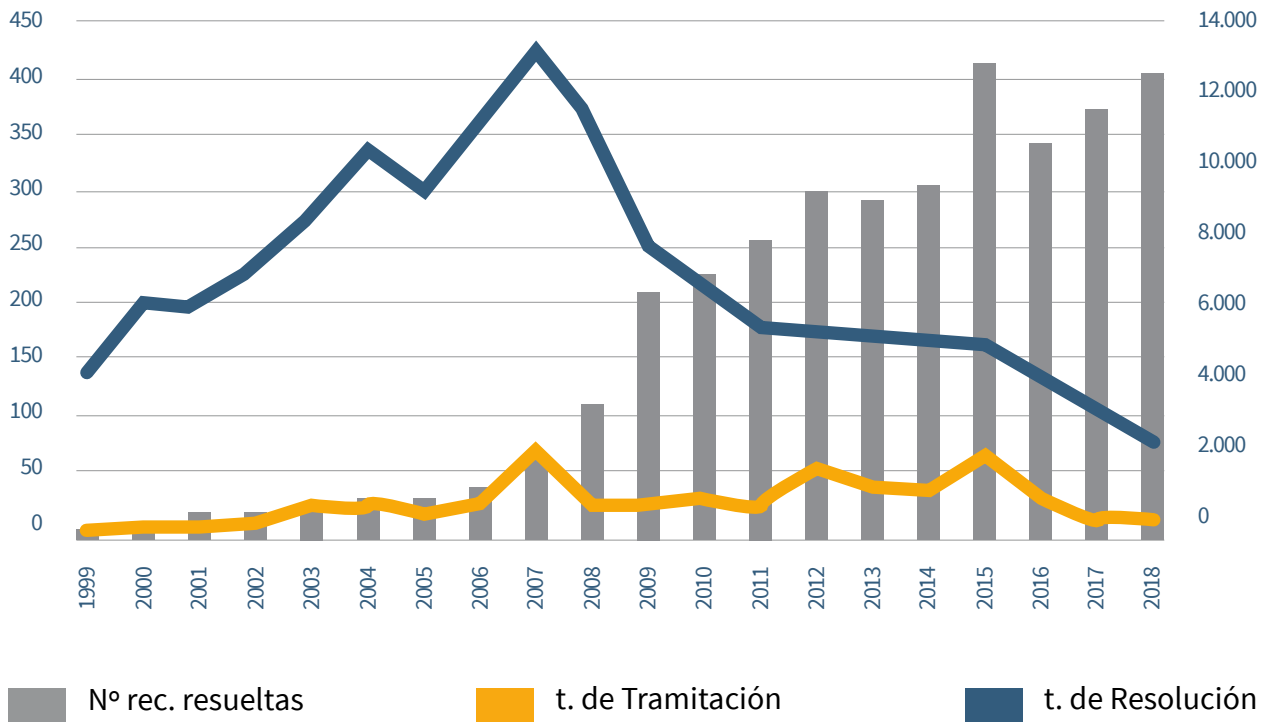
***Se incluyen en este epígrafe las notificaciones de brechas de seguridad que son analizadas por la UEET sin dar lugar a actuaciones de investigación por parte de la SDG de Inspección.

► Eficacia administrativa

Se reflejan tiempos medios de tramitación (en días) desde que se registra la denuncia o se abren actuaciones de oficio hasta que se dicta resolución.

Tiempos medios de tramitación					
	2016	2017	2018	Δ% 2017/2018	Δ% 2016/2018
Archivo de denuncia sin actuaciones de investigación	64	23,7	19,6	-17%	-69%
Resolución de reclamación tras traslado al delegado o responsable	-	-	76	-	-
Archivo de actuaciones tras no subsanarse denuncia	83	70,99	-	-	-
Archivo de actuaciones de investigación	323	268,88	176,96	-34%	-45%
Resolución de procedimientos de apercibimiento	267	239,05	-	-	-
Resolución de procedimientos sancionadores	507	399,68	296,83	-26%	-41%
Resolución de procedimientos de infracción de las AAPP	477	410,81	-	-	-
Resolución de procedimientos de tutela de derechos	120	98,57	85,93	-13%	-28%

Reclamaciones resueltas



t. de Tramitación: desde que llega una entrada hasta que se comienza un procedimiento.
 t. de Resolución: desde que llega una entrada hasta que se resuelve.

► Tutela de derechos

Resoluciones - Tutela de derechos

	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Estimatoria	371	438	401	43%	-8%	8%
Estimatoria formal o parcial	270	368	245	26%	-33%	-9%
Desestimatoria	433	402	281	30%	-30%	-35%
TOTAL	1074	1208	927	100%	-23%	-13%

Distribución de derechos tutelados según resultado de la resolución

	Estimatoria	Estimatoria total o parcial	Desestimatoria	TOTAL
Cancelación (excepto derecho al olvido)	150	128	143	567
Derecho al olvido	43	31	72	146
Acceso	174	69	52	295
Rectificación	12	5	0	17
Oposición/exclusión	22	12	14	48
TOTAL	401	245	281	927

► Sanciones

Evolución de las infracciones con sanción económica

	2016	2017	2018	$\Delta\%$ 2017/2018	$\Delta\%$ 2016/2018
*Total sanciones	560	694	371	-47%	-34%

*En los procedimientos sancionadores que se rigen por el RGPD (reclamaciones posteriores al 25 de mayo) aún no se han impuesto sanciones económicas.

Áreas con mayor importe global de sanciones						
	2016	2017	2018	% relativo	Δ% 2017/2018	Δ% 2016/2018
Contratación fraudulenta	3.420.000	3.328.401	5.003.200	43%	50%	46%
Ficheros de Morosidad	5.835.007	6.318.008	3.842.804	33%	-3%	-34%
Directorios	-	-	1.074.002	9%	-	-
Servicios de Internet	-	2.146.440	742.400	6%	-65%	-
Reclamación de deudas	1.065.801	1.152.104	626.801	5%	-46%	-41%
Publicidad (excepto spam)	1.964.305	2.695.382	406.700	3%	-85%	-79%
% relativo al total del año	90%	72%	89%	-	-	-1%
TOTAL (6 primeras)	12.724.967	12.311.934	11.695.907	100%	-5%	-8,09%

	2016	2017	2018	Δ% 2017/2018	Δ% 2016/2018
* Importe Total sanciones	14.190.173	17.319.962	13.180.655	-24%	-7%

*El 79% de las sanciones impuestas en el 2018 se han satisfecho con las reducciones de reconocimiento de responsabilidad y pronto pago que faculta la Ley 39/2015.

► Áreas de actividad

Reclamaciones planteadas con mayor frecuencia					
	2016	2017	2018	% relativo	Δ% 2017/2018
Ficheros de Morosidad	2.197	2.263	2.127	16%	-6%
Videovigilancia	1.229	1.269	1.396	11%	10%
Servicios de Internet	890	864	1.353	10%	57%
Reclamación de Deudas	-	918	1.261	10%	37%
Administración pública	532	650	957	7%	47%
Sanidad	379	361	901	7%	150%
Publicidad (excepto spam)	419	406	644	5%	59%
Comercios, transporte y hostelería	222	292	606	5%	108%
Entidades financieras/acreedoras	960	482	576	4%	20%
Publicidad a través de e-mail o teléfono móvil	333	378	483	4%	28%

Áreas más frecuentes en procedimientos sancionadores					
Videovigilancia	378	395	260	32%	-34%
Contratación fraudulenta	87	98	107	13%	9%
Ficheros de Morosidad	165	229	105	13%	-54%
Servicios de Internet	41	56	55	7%	-2%
Publicidad a través de e-mail o teléfono móvil	97	75	52	6%	-31%
Publicidad (excepto spam)	66	97	44	5%	-55%
Asuntos laborales	4	12	26	3%	117%
Artículo 5 Internet	43	32	24	3%	-25%
Comercios, transporte y hostelería	10	15	16	2%	7%
Reclamación de Deudas	-	5	16	2%	220%

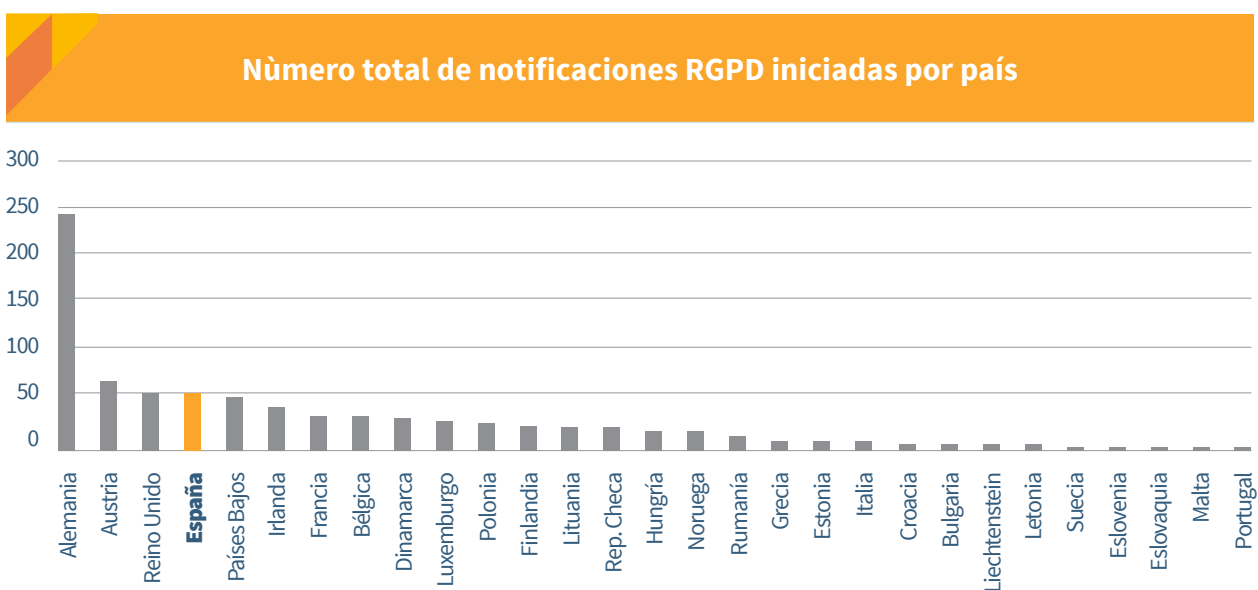
► Cooperación RGPD

Cooperación transfronteriza	
	2018
Casos transfronterizos liderados por la AEPD	15
Casos transfronterizos en seguimiento como AC interesada	229
Solicitudes de asistencia mutua y consultas recibidas de otras AC europeas	24
Resoluciones transfronterizas revisadas como AC interesada	9
TOTAL	262

Notificaciones RGPD iniciadas por país	
País	2018
Alemania	244
Austria	57
Reino Unido	51
España	50
Países Bajos	48
Irlanda	30
Francia	21
Bélgica	20
Dinamarca	19
Luxemburgo	17
Polonia	14
Finlandia	12
Lituania	10

República Checa	10
Hungría	9
Noruega	8
Rumania	5
Grecia	3
Estonia	3
Italia	3
Croacia	2
Bulgaria	2
Liechtenstein	2
Letonia	2
Suecia	1
Eslovenia	1
Eslovaquia	1
Malta	1
Portugal	1

Comprende nuevos procedimientos. Art. 56 (Identificación de LSA y CSA), 60 (DD, RDD, FD, IC) y 64 (Opinión del EDPB).



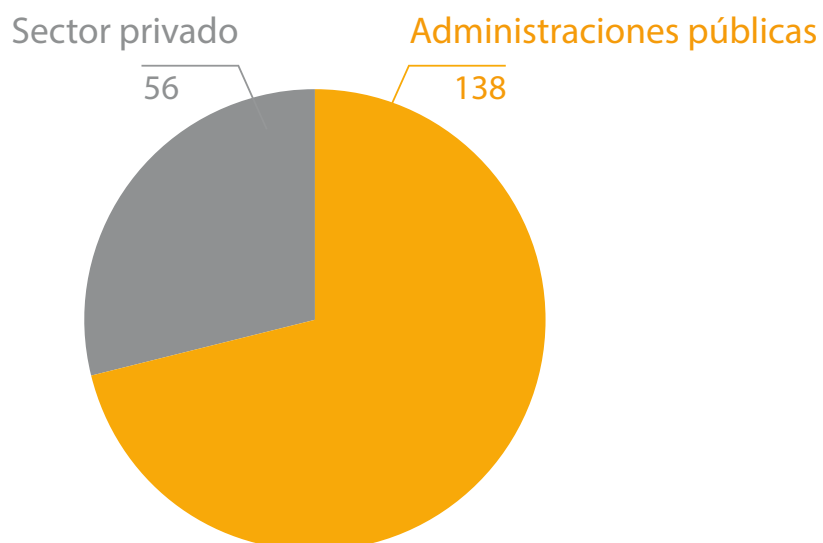
4. Gabinete jurídico

Consultas

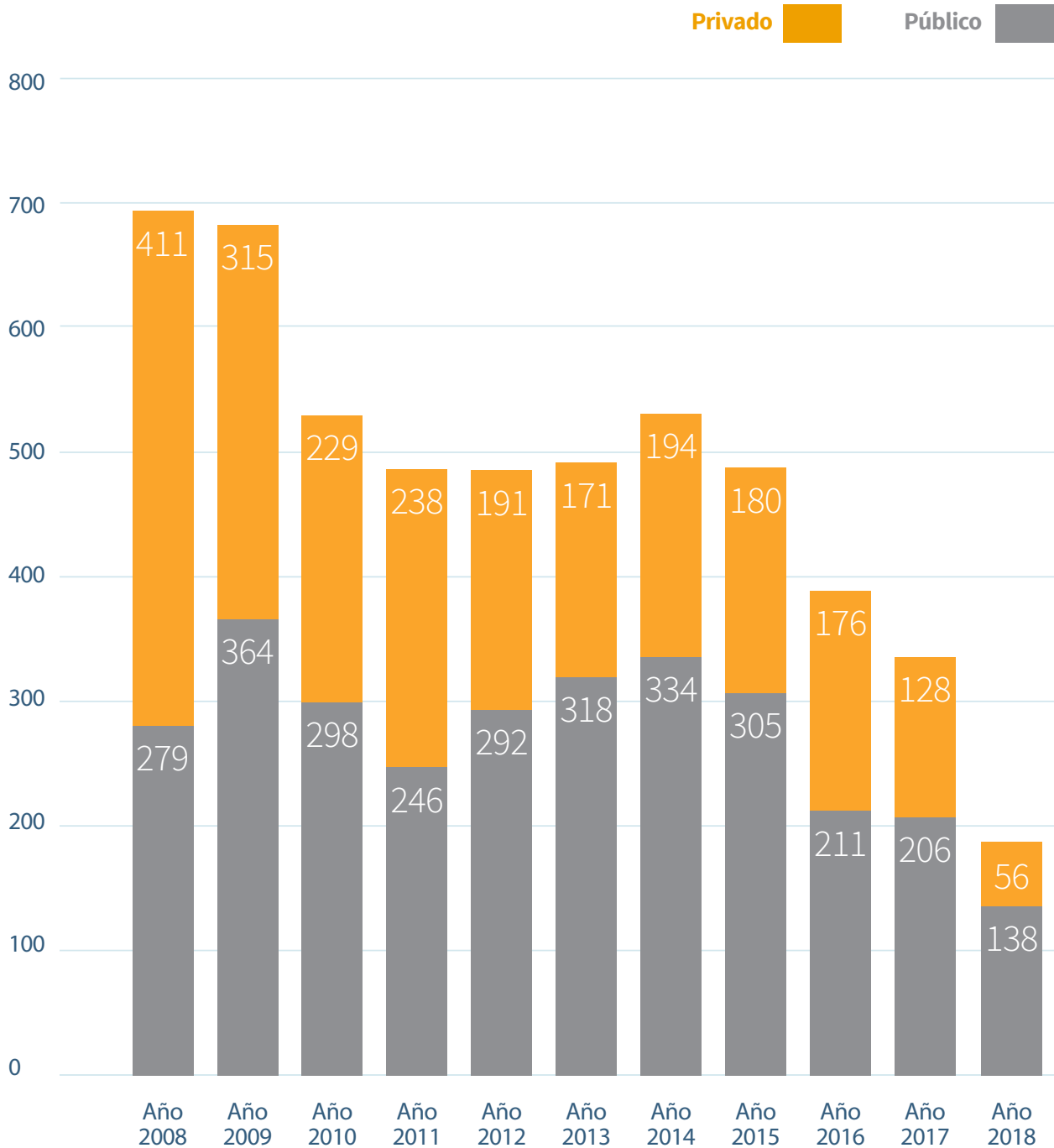
Administraciones públicas	
Administración General del Estado	81
Comunidades Autónomas	20
Entidades Locales	7
Otros Organismos	30
TOTAL	138

Consultas privadas	
Asociaciones y Fundaciones	5
Empresas	44
Particulares	3
Sindicatos	3
Otros	1
TOTAL	56

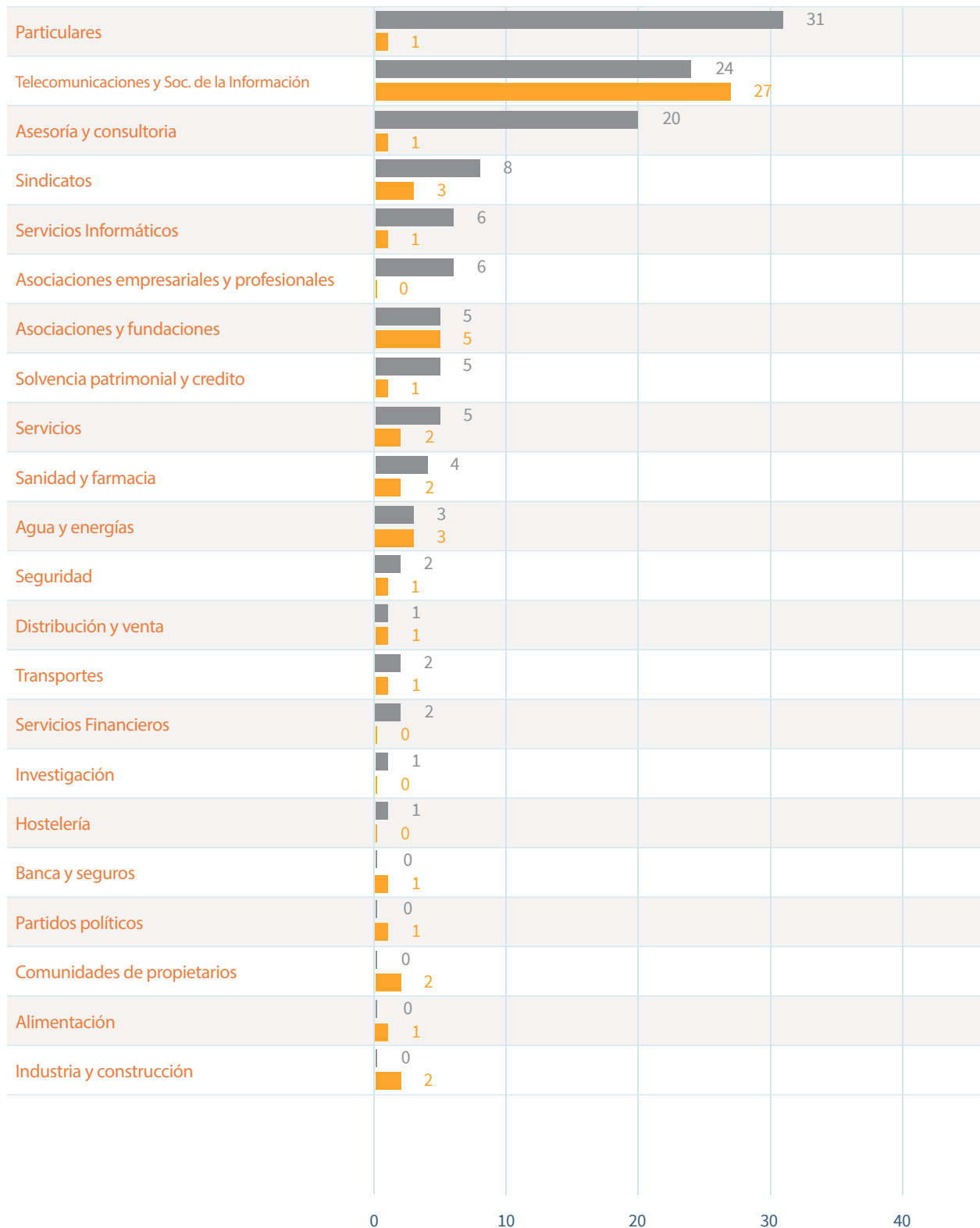
Distribución 2018 de consultas públicas/privadas



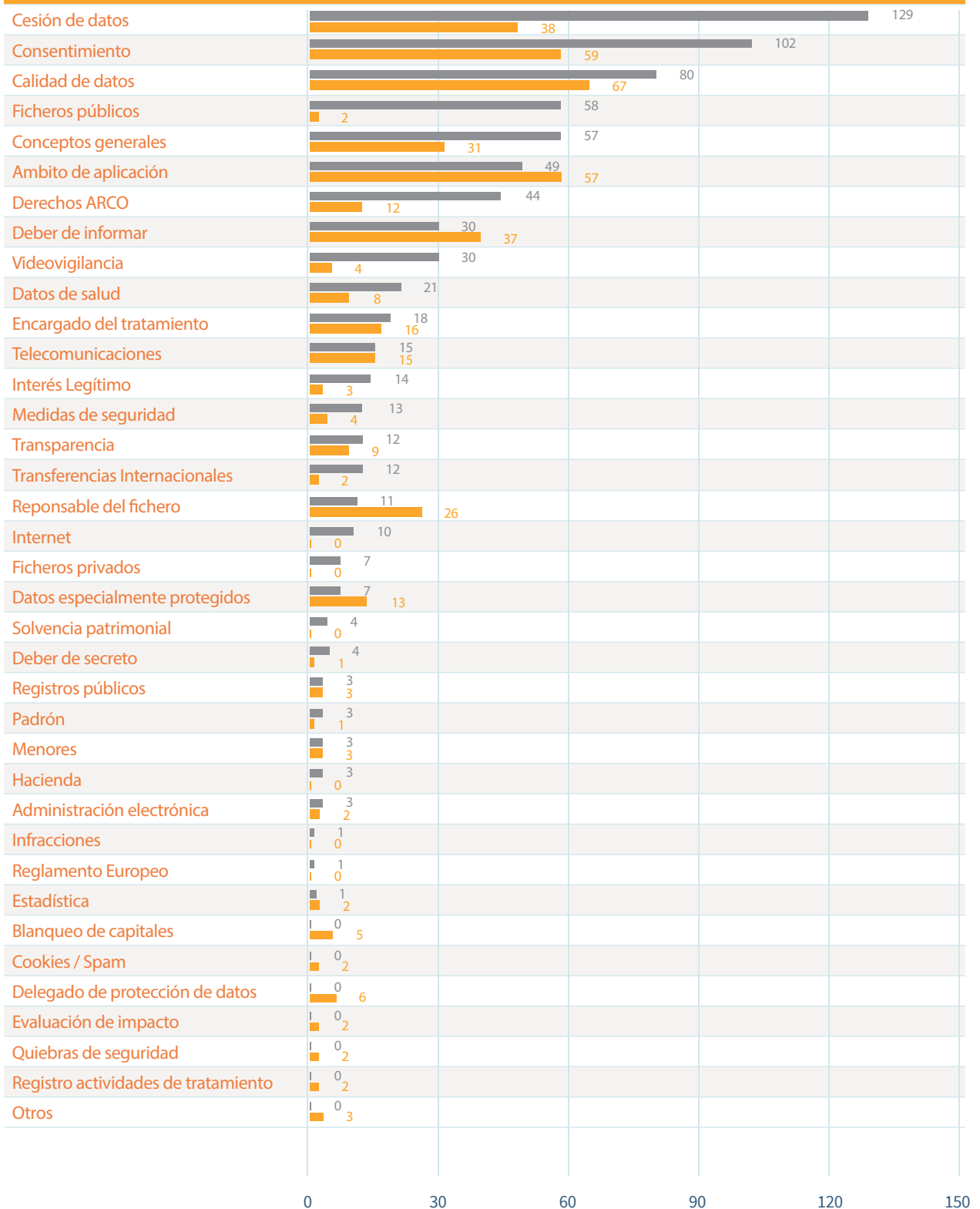
Evolución de las consultas (2007-2017)



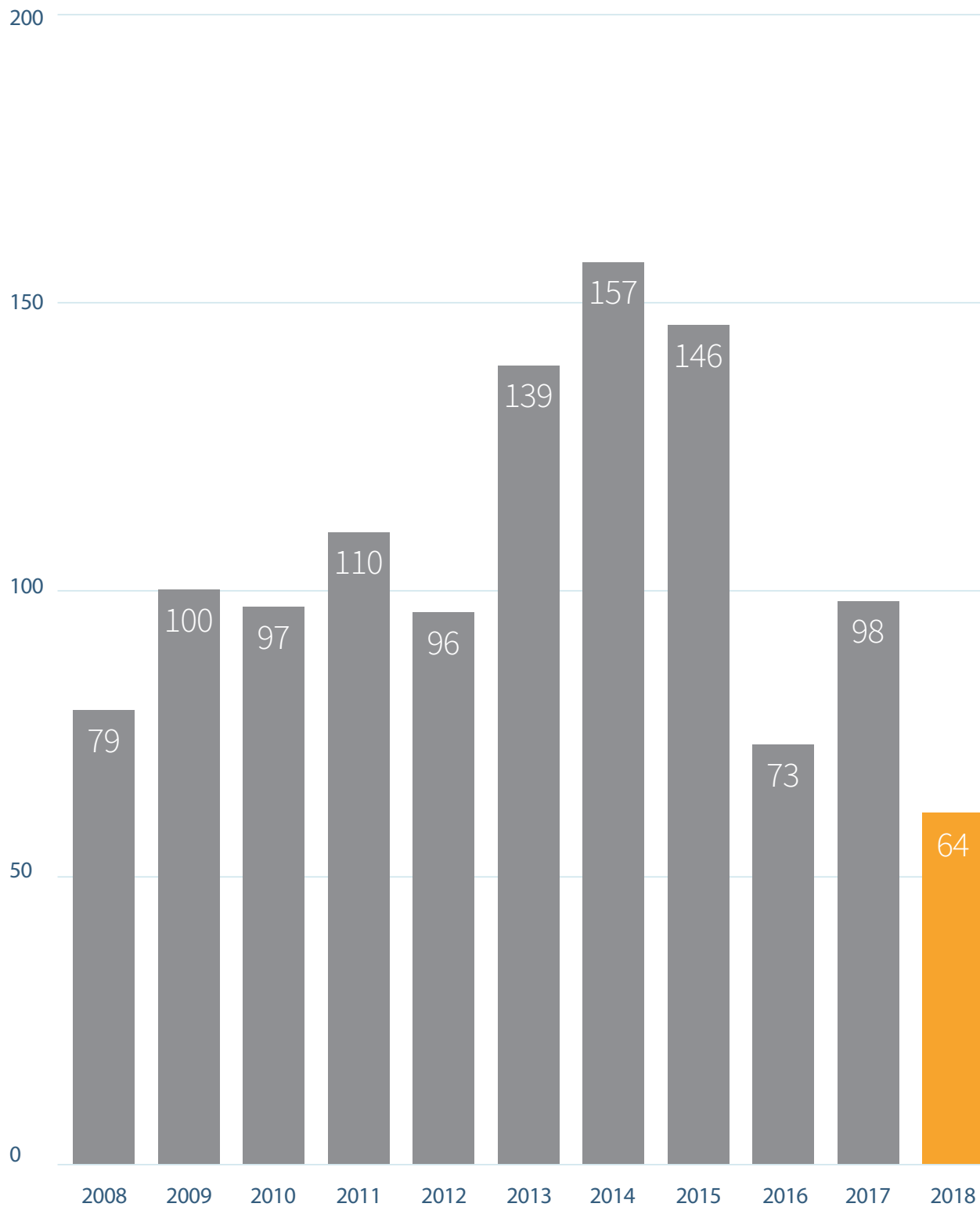
Evolución de consultas por sectores (2017 ■ 2018 □)



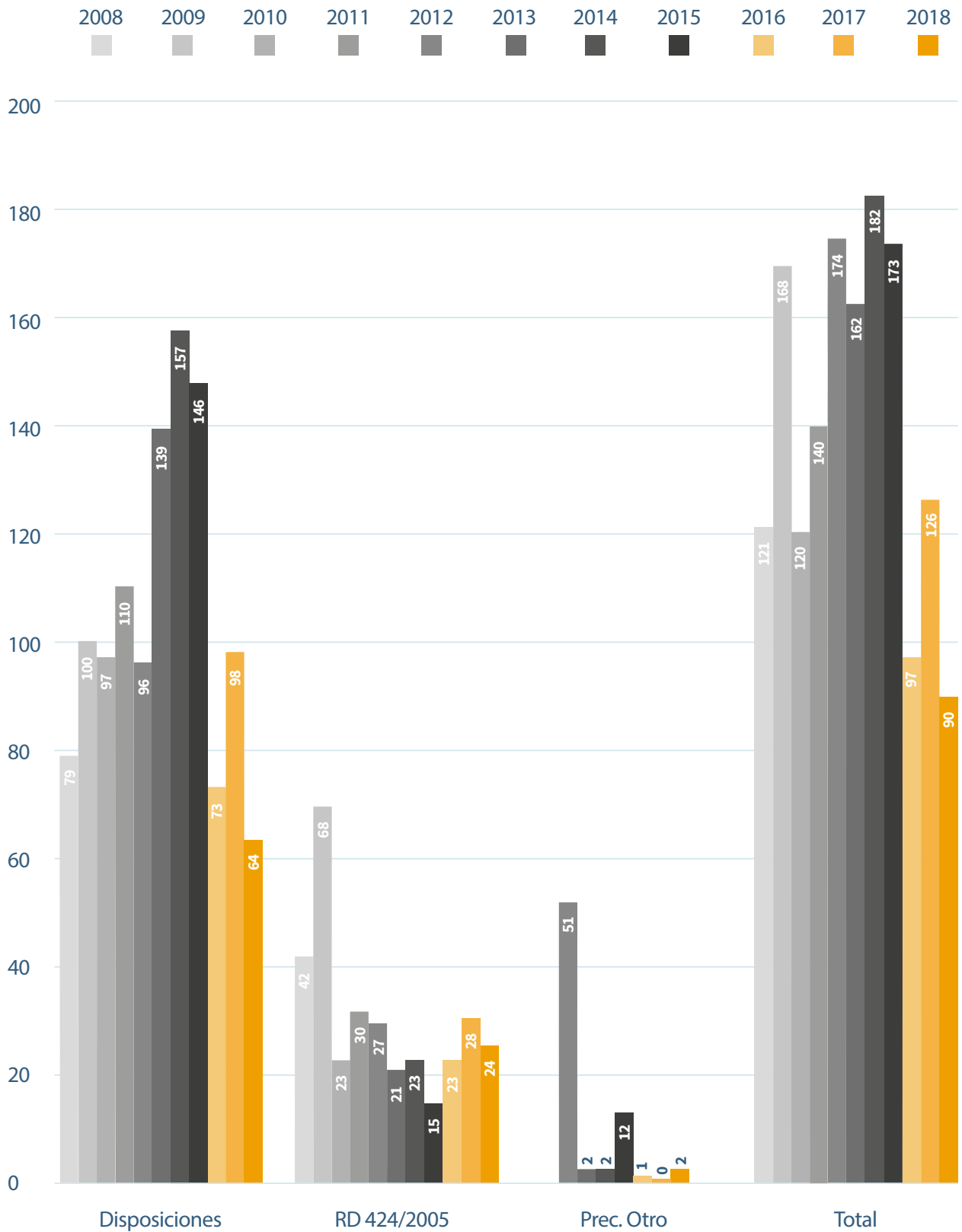
Evolución de consultas por materias (2017 ■ 2018 □)



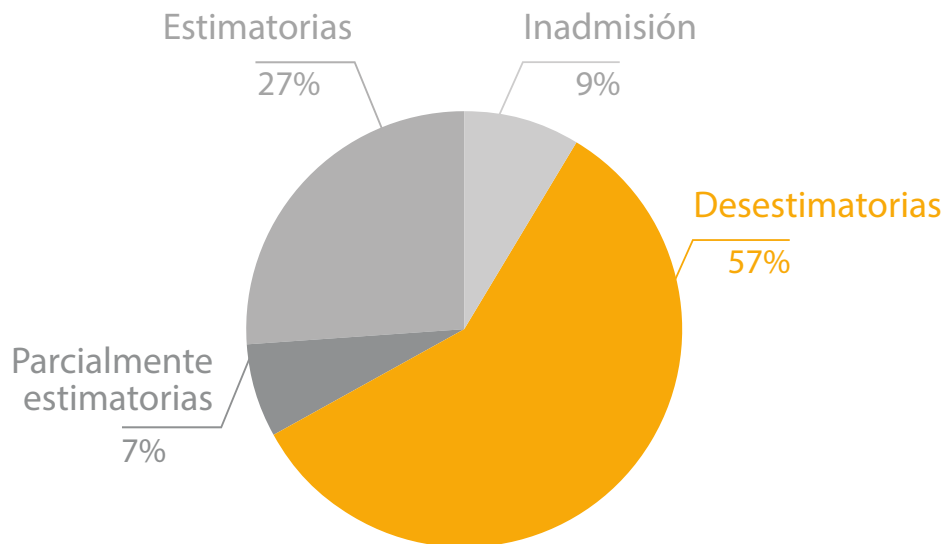
Evolución de informes preceptivos a disposiciones generales (2008-2018)



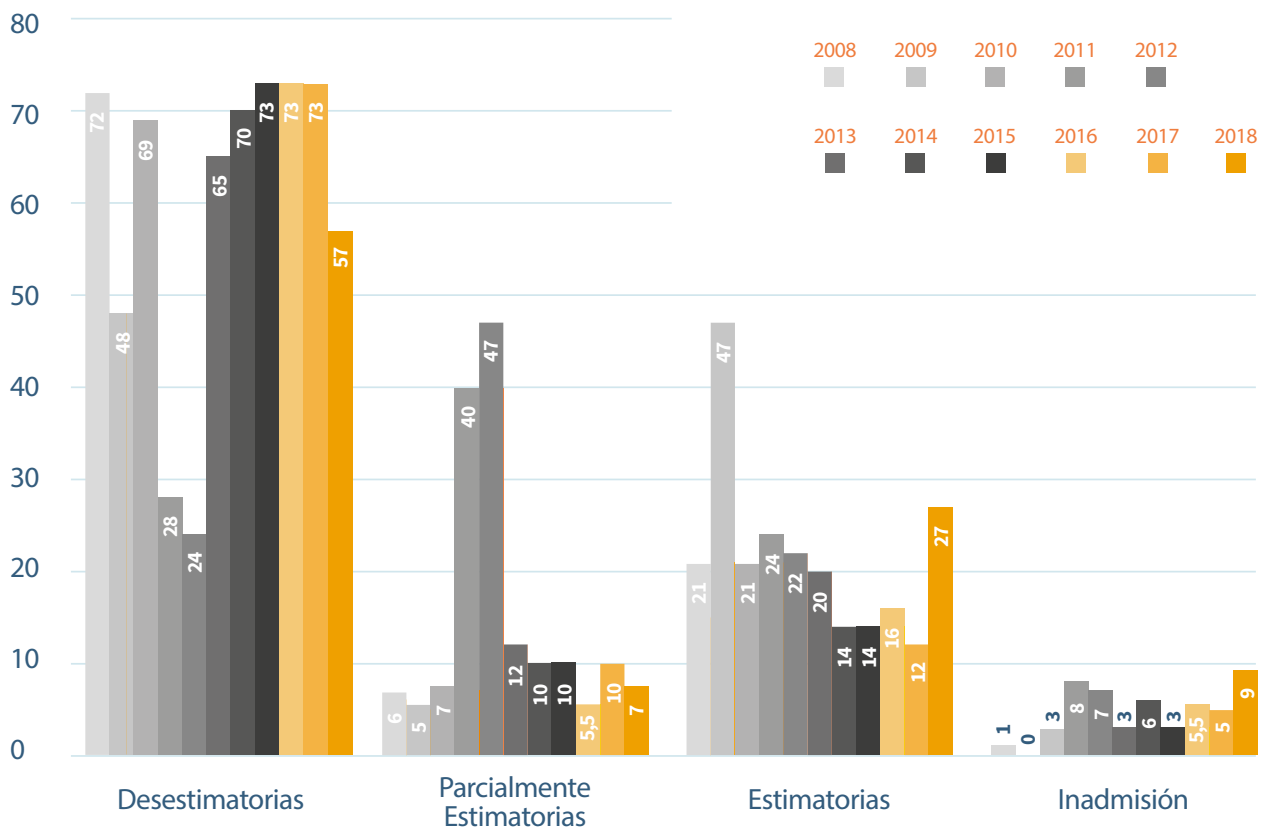
Evolución de informes preceptivos (2008-2018)



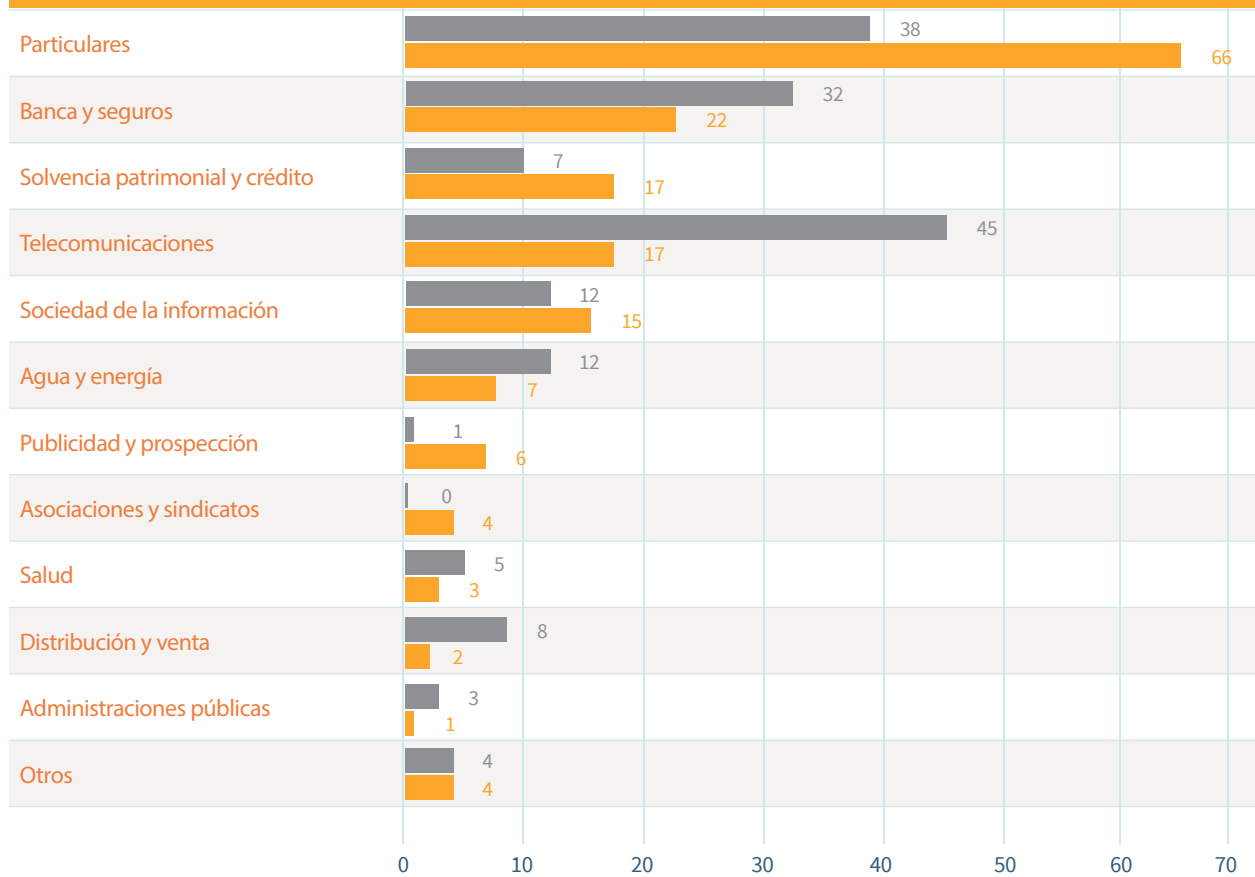
Sentencias Audiencia Nacional en 2018



Evolución por sentido del fallo en porcentajes (2008-2018)



Comparativa por sector del recurrente (2017 ■ 2018 □)



5. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano				
	2016	2017	2018	% 2017 - 2018
Presenciales	4.183	3.699	3.455	-6,95
Telefónicas	76.869	73.501	88.302	+20,13
FAQs	147.297	170.754	651.650	+281,63
Escritas	8.606	7.954	5.613	-29,43
Correo	552	516	453	-12,2
Buzón sede electrónica	8.054	7.438	5160	-30,62
TOTAL	236.955	255.298	-6,52	+192,69

Comparativa de visitas a la web (www.aepd.es)				
	2016	2017	2018	% 2017 - 2018
Visitas	5.534.282	6.724.113	7.925.300	+17,86%

Consultas especializadas sobre el tratamiento de datos de menores				
	2016	2017	2018	% 2017 - 2018
Teléfono	218	178	597	+235,39
WhatsApp	157	247	384	+55,47
Correo electrónico	200	246	388	+57,72
Sede electrónica	229	224	195	-12,95
TOTAL	804	895	1.564	+74.75%

Accesos a los vídeos “Protege tus datos en internet”

	2017	2018	%
Accesos al canal	29.672	34.347	+15,75
Visualizaciones de vídeos	33.283	334.455	+904,88

*Se puede acceder a los vídeos directamente a través de la web “tudecideseninternet.es”

Accesos a la web www.tudecideseninternet.es

	2017	2018	%
*Visitantes distintos	66.810	121.998	+82,60
**Visitas	101.500	169.689	+67,18

* Visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo cuenta como una.

** Número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumenta este contador.

Canal INFORMA_RGPD

	Consultas
*Canal INFORMA_RGPD	4.116

*El canal Informa_RGPD se lanzó en marzo de 2018.

Temas más consultados en el catálogo de preguntas frecuentes (FAQs)

Orden	Temas de consulta	Accesos
1	Delegados de protección de datos y certificación	65.427
2	Comunidades de propietarios	57.225
3	Videovigilancia	52.052
4	En qué te podemos ayudar y en qué no	45.794
5	Reglamento General de Protección de Datos (RGPD)	44.324
6	Solvencia patrimonial	44.065
7	Ficheros: inscripción, modificación, supresión y novedades del RGPD	32.322
8	Tratamiento de datos en el ámbito laboral	28.366
9	Aspectos técnicos Sede electrónica	24.669
10	Obligaciones de los responsables de ficheros	20.633

Temas más consultados en la atención presencial y telefónica

Orden	Temas de consulta	%
1	Reglamento General de Protección de Datos	29,09
2	Reclamaciones	12,96
3	Herramienta FACILITA	6,96
4	Solvencia patrimonial	6,56
5	Videovigilancia	5,97
6	Ficheros: inscripción, modificación, supresión y novedades del RGPD	5,35
7	Obligaciones de los responsables de ficheros	2,99
8	Delegados de protección de datos	2,66
9	Cesiones de datos	1,71
10	Otras cuestiones	9,38

Consultas telefónicas y presenciales sobre derechos

Derechos	%
Cancelación	14,8
Acceso	13,43
Olvido	4
Oposición	2,89
Rectificación	0,91
Requisitos para su ejercicio	1,77
Derechos RGPD	62,19

Herramienta FACILITA

	2017	2018
Accesos a Facilita_RGPD	29.009	622.550
Cuestionarios finalizados	6.196	150.360

Otros contenidos

Guías generales	Descargas
Guía sobre el uso de videocámaras para seguridad y otras finalidades	33.990
Guía para la gestión y notificación de brechas de seguridad	25.868
Protección de datos: guía para el ciudadano	232.982
Listado de elementos para el cumplimiento normativo	62.452
Guía para el responsable de tratamiento de datos personales	221.099
Guía práctica de análisis de riesgos en tratamientos de datos personales sujetos al RGPD	159.007
Guía de evaluación de impacto en la protección de datos personales	122.442
Guía para el cumplimiento del deber de informar	106.124

Otros contenidos

Guías generales	Descargas
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	66.933
Guías sectoriales	
Guía de administradores de fincas	18.737
Compra segura en INTERNET - Guía Práctica	99.531
Guía de Privacidad y Seguridad en Internet	179.216
Protección de datos y Administración Local	55.602
Guía de protección de datos y prevención de delitos	26.434
Guía de protección de datos y prevención de delitos: fichas prácticas	11.409
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube	106.124
Código de buenas prácticas en protección de datos para proyectos. Big Data	20.284
Cómo gestionar una fuga de información en un despacho de abogados	5.758
Orientaciones y Garantías en los procedimientos de anonimización	15.529
Guía para clientes que contraten servicios de Cloud Computing	3.428
Orientaciones para prestadores de servicios de Cloud Computing	1.333
Estudios	
LOPDPDGG: Novedades para los ciudadanos	1.394
LOPDPDGG: Novedades para el Sector Privado	1.885
LOPDPDGG: Novedades para el Sector Público	1.079
25 años de la Agencia Española de Protección de Datos	1.926
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	9.494
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	6.359
Encuesta: grado preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	2.029

Otros contenidos

Infografías	Descargas
Compra segura en internet	3.047
Juguetes conectados	2.042
Cómo evitar la publicidad no deseada	32.590
Los derechos que tienes para proteger tus datos personales	42.535
Adaptación al RGPD de las Administraciones Públicas	67.218
Adaptación al RGPD del Sector Privado	70.017
Decálogo para el personal sanitario y administrativo	78.907
Memorias	
Memoria 2017	4.196

Solicitud de copia de contenido de la inscripción de ficheros como ayuda para elaborar el Registro de actividades de Tratamiento

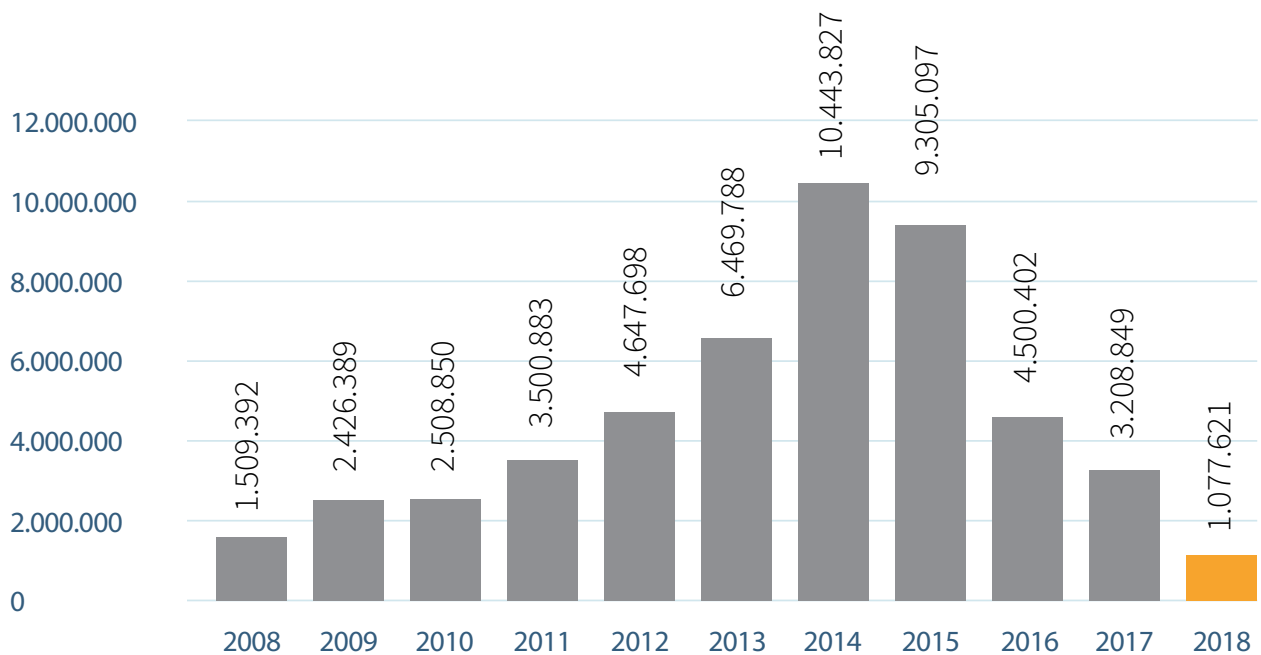
		Nº expedientes	Días en responder
Recibidas en papel	Tit. Privada	126	4
	Tit. Pública	21	
Correo postal, fax o mano	Tit. Pública		
Sede electrónica AEPD	Tit. Privada firmada	10.400	7
	Tit. Privada sin firma	1.783	
	Tit. Pública firmada	454	
	Tit. Pública sin firma	35	

Registro de delegados de protección de datos comunicados

Titularidad	Total Comunicados
Entidades privadas	17.296
Entidades públicas	2.747
	Administración General del Estado 85
	Comunidades Autónomas 243
	Entidades Locales 1.215
	Otras personas Jurídico-Públicas
	· Consejo General del Poder Judicial
	· Notarios
	· Colegios Profesionales
	· Universidades
	· Cámaras de Comercio
	· Comunidades de Regantes...
TOTAL	20.043

6. Registro General de Protección de Datos (operativo hasta mayo de 2018)

Derecho de consulta		
Titularidad ficheros	2017	2018
Privada	2.341.761	941.204
Pública	867.088	136.417
TOTAL	3.208.849	1.077.621



Evolución de la inscripción de ficheros								
A 31 de diciembre	2011	2012	2013	2014	2015	2016	2017	2018
Tit. Pública	117.503	137.396	146.282	152.824	157.324	161.892	166.501	168.499
Tit. Privada	2.491.968	2.865.720	3.228.777	3.594.106	3.950.620	4.348.454	4.748.433	4.925.814
TOTAL	2.609.471	3.003.116	3.375.059	3.746.930	4.107.944	4.510.346	4.914.934	5.094.313

7. Transferencias internacionales de datos

Resoluciones de autorización concedidas en aplicación de la LOPD 5/1999.

País	TOTAL AUTORIZACIONES
Estados Unidos	966
Panamá	9
Colombia	176
Chile	49
Uruguay	25
Perú	155
Guatemala	6
Paraguay	17
Iberoamérica	
Brasil	24
El Salvador	2
Costa Rica	18
Nicaragua	1
México	102
Ecuador	1
Venezuela	1
India	356
Marruecos	86
Singapur	37
Otros Países	
Japón	37
Malasia	23
Tailandia	7

País	TOTAL AUTORIZACIONES
Filipinas	72
China	49
Hong Kong	17
Egipto	6
Nigeria	1
Túnez	9
Sudáfrica	11
Australia	32
Canadá	9
República Bielorrusa	3
Mónaco	1
Israel	9
Otros Países	
Vietnam	4
Barbados	3
Andorra	1
Mauricio	2
Kenia	1
Serbia	11
Taiwán	4
Croacia	1
Turquía	3
Ucrania	3
Bermudas	3
Nueva Zelanda	2
República de Corea	4

País	TOTAL AUTORIZACIONES
Federación Rusa	9
Emiratos Árabes	4
Arabia Saudí	6
Indonesia	2
Puerto Rico	2
Irán	1
Otros Países	
Qatar	1
Camboya	1
Myanmar	1
Botsuana	1
Madagascar	1
República de Moldova	2
Rep. Democrática Pop. de Laos	1
Internacional	73
Solicitudes presentadas	2.899
Archivadas	649
TOTAL AUTORIZACIONES	2.169

Ficheros inscritos con transferencias internacionales según titularidad	
	Ficheros
Titularidad Privada	20.928
Titularidad Pública	8.457
TOTAL	29.385

Evolución de las autorizaciones de transferencias internacionales según las garantías aportadas (tipo de contrato y normas corporativas vinculantes -BCR-)

	2001/497/CE ¹	2002/16/CE ² 2010/87/UE ³	BCR ⁴	Cláusulas Encargado - Subencargado	Contrato ad hoc
2010	80	475	-	-	-
2011	112	619	1	-	-
2012	167	735	8	2	-
2013	195	861	17	9	-
2014	226	966	23	16	1
2015	246	1.037	34	22	1
2016	379	1.364	61	32	2
2017	434	1.527	83	43	3
2018	443	1.586	88	48	4

Actuaciones en la adopción de Normas Corporativas Vinculantes (BCR)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	TOTAL
Revisión BCR'S	1	4	7	3	9	10	8	7	14 ⁵	63

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 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.

⁵ La AEPD actúa como autoridad líder en 2 BCR.

8. Secretaría General

Solicitudes de acceso a la información pública					
Recibidas	Concedidas	Inadmitidas*	Desistimiento	Consultas**	Denegadas
118	84	7	0	24	3

* Abuso de derecho (1); en elaboración o pendiente de publicar (1); la información no obraba en poder de la AEPD (5)

** No eran peticiones de acceso a la información, sino consultas sobre protección de datos.

► Gestión de Recursos Humanos

	Dotación	Cubiertos
Funcionarios	180	151
Laborales	4	2
Laborales fuera de Convenio	2	2
Alto cargo	1	1
TOTAL	187	156
	MUJERES 78	HOMBRES 78

► Funcionarios

NIVEL	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	6	3	27	54	-	16	2	13	2	7	10	11

GRUPO	A1	A2	C1	C2
Efectivos	38	53	22	38

Evolución del presupuesto

	Crédito ejercicio 2016	Crédito ejercicio 2017	Crédito ejercicio 2018
Capítulo I	7.305.820	7.360.820	7.986.570
Capítulo II	4.896.060	4.956.060	5.071.756
Capítulo III	232.450	160.950	80.950
Capítulo IV	267.940	284.440	284.440
Capítulo VI	1.316.000	1.316.000	937.860
Capítulo VIII	22.800	22.800	22.800
TOTAL	14.101.070	14.101.070	14.384.376

* Los datos de todos los capítulos son siempre referidos a créditos definitivos.

9. Presencia internacional de la AEPD

Reunión	Fecha	Lugar
Sesiones Plenarias del Grupo de Trabajo del Artículo 29 (GT29)	6 y 7 de febrero 10 y 11 de abril	Bruselas (Bélgica)
Sesiones Plenarias del Comité Europeo de Protección de Datos (CEPD)	24 y 25 de mayo 4 y 5 de julio 25 y 26 de septiembre 25 y 26 de noviembre 16 de noviembre 4 y 5 de diciembre	

Reuniones de subgrupos del Comité Europeo de Protección de datos

* Reuniones de subgrupos pertenecientes al GT29 (anteriores a la creación del CEPD)

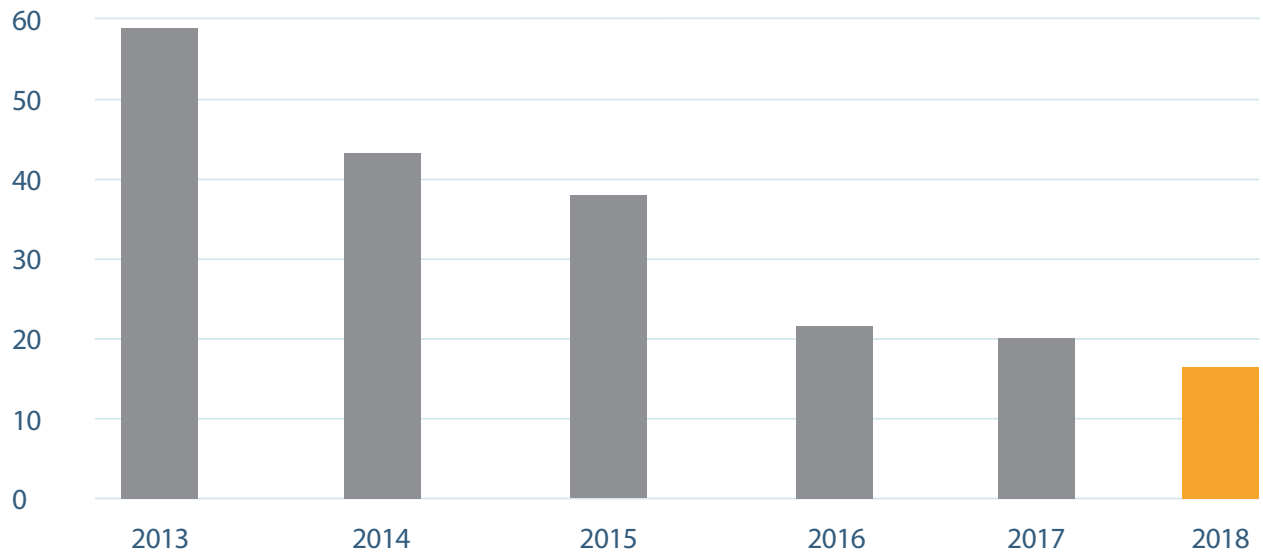
Reunión	Fecha	Lugar
Reunión de coordinación de subgrupos	6 de marzo* 15 de junio 10 de septiembre	Bruselas (Bélgica)
Futuro de la privacidad (FoP)	19 de enero* 20 de marzo* 19 de junio 11 de septiembre	
Supervisión del cumplimiento (enforcement)	15 de enero* 8 de marzo* 8 de mayo 6 de septiembre 12 de noviembre	
Cooperación	11 de enero* 7 y 8 de marzo* 16 de mayo 5 de septiembre 13 y 14 de noviembre	
Multas	9 de marzo* 16 de mayo 7 de septiembre 15 de noviembre	
Asuntos financieros	17 y 18 de enero* 20 de marzo* 17 y 18 de abril* 18 de julio 15 de noviembre	
Fronteras, viajeros y supervisión del cumplimiento (BTLE)	10 de enero* 15 de marzo* 26 de abril* 26 de junio 6 de septiembre 30 de octubre 18 de diciembre	

Reunión	Fecha	Lugar
Gobierno electrónico (E-Government)	19 de enero* 22 de marzo* 2 de mayo 13 de septiembre 18 de octubre 19 y 20 de noviembre	Bruselas (Bélgica)
Transferencias Internacionales	12 de junio 10 de julio 16 y 17 de octubre 12 de noviembre 11 y 12 de diciembre	
Tecnología	17 de enero* 22 de marzo* 23 y 24 de abril* 14 de junio 4 y 5 de septiembre 6 y 7 de noviembre 19 de diciembre	
Plataformas Sociales	15 de mayo 14 de septiembre 9 de noviembre	
Reuniones de subgrupos de redacción de las Reglas de Procedimiento del Comité Europeo de Protección de Datos (CEPD)	12 de enero 27 de marzo 17 de abril	
IMI - Grupo de trabajo y evento formativo	9 de febrero 23 de marzo 27 de abril	
Control de Agencias y Grandes Sistemas de Información UE		
Comité de Cooperación EUROPOL	30 de mayo 3 de octubre	Bruselas (Bélgica)
Grupos de Supervisión Coordinada de los sistemas VIS, SIS II y EURODAC	12 y 13 de junio 14 y 15 de noviembre	
Sistema de información aduanera	29 de mayo 2 de octubre	
Consejo de Europa- 46ª Reunión la Oficina del Convenio 108	17 al 19 de diciembre	Estrasburgo (Francia)
Evaluación Schengen Letonia	15 al 20 de abril	Riga (Letonia)
Control de Agencias y grandes sistemas de información	7 y 8 de junio	Amsterdam (Países Bajos)

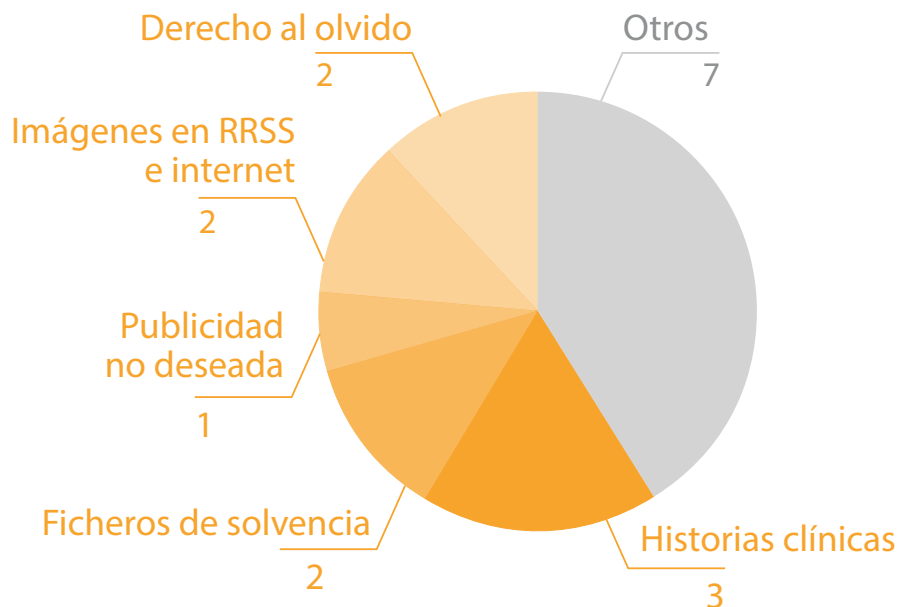
Reuniones y conferencias internacionales

Reunión	Fecha	Lugar
PROYECTO T4DATA - Formación para autoridades de protección de datos y encargados de protección de datos:		
Primera reunión de colaboradores del proyecto T4DATA	12 al 14 de marzo	Zagreb (Croacia)
Primera formación transnacional para APD	10 al 14 de junio	Roma (Italia)
Segunda formación transnacional para formadores y reunión organizativa de colaboradores	7 al 12 de octubre	Varsovia (Polonia)
CGPJ - Protección datos en víctimas de delitos	9 al 13 de diciembre	Estambul (Turquía)
Conferencia Internacional de Autoridades de Protección de datos y Privacidad	22-24 de octubre	Sofía (Bulgaria)
Conferencia Anual ICANN 63	22 y 24 de octubre	Barcelona
Conferencia Implementación RGPD	30 de abril y 1 de mayo	Londres (Reino Unido)
40 Conferencia internacional de autoridades de protección de datos y privacidad	22 al 25 de octubre	Bruselas (Bélgica)
Grupo de trabajo Whatsapp	25 de enero	Londres (Reino Unido)
Grupo de trabajo Google	27 de febrero	París (Francia)
Grupo de trabajo Uber	14 de febrero	La Haya (Países Bajos)
GPEN- Grupo de trabajo para aplicación normativa	13 al 15 de Junio	Tel Aviv (Israel)
Grupo Internacional de Protección de Datos en Telecomunicaciones (Grupo de Berlín)	10 de abril	Budapest (Hungria)

10. Defensor del Pueblo



Materias





www.aepd.es