aepd agencia española protección datos

MEMORIA ANUAL 2022

prólogo

La Memoria que tengo el honor de presentar ofrece una exposición detallada de las actividades puestas en marcha durante el año 2022, junto a un análisis de las tendencias normativas y jurisprudenciales y los retos de futuro en relación con la protección de datos personales. Las siguientes páginas son el reflejo de cómo una autoridad de supervisión tiene la obligación de trabajar de forma simultánea en diversos planos para conseguir los objetivos que se ha propuesto: desde la concienciación ayudando a aquellos que tratan datos a cumplir con sus obligaciones y prestando ayuda a los ciudadanos, como ejerciendo sus potestades cuando es necesario.

La Agencia tiene entre sus objetivos principales fomentar una cultura de protección de datos. Teniendo en cuenta el imparable avance de la digitalización y las nuevas tecnologías en un mundo globalizado, durante el año 2022 hemos seguido profundizando en una de las misiones que mayor impacto tiene en el ciudadano: la protección de las personas en un mundo digital. Ello conlleva prestar especial atención a los avances tecnológicos y parte de la actividad de este organismo se ha centrado en la elaboración de más de una veintena de guías, modelos, estudios y notas con recomendaciones para las organizaciones que tratan datos.

Nos encontramos en una etapa decisiva en la que fomentar la protección de los datos personales es imprescindible para garantizar, por un lado, una innovación sostenible y, por otro, la libertad de las personas ante la expansión de unos tratamientos de datos que pueden llegar a ser extremadamente intrusivos. La biometría, la inteligencia artificial, el big data o el internet de las cosas, entre otros, son avances positivos que tienen que desarrollarse conforme a los derechos fundamentales para no terminar convirtiéndose en amenazas. Es necesario trabajar con aquellos que tratan datos personales, de forma que utilicen todos los recursos gratuitos que ponemos a su disposición y que han supuesto el lanzamiento de más de 100 guías y herramientas adaptadas al Reglamento General de Protección de Datos en los últimos años. En ese marco, hay que mencionar la importancia de la figura del delegado de protección de datos. En 2022 se han superado los 100.000 DPDs notificados, y casi 3.000 de las reclamaciones recibidas se han trasladado al responsable o encargado del tratamiento obteniendo una respuesta satisfactoria para el ciudadano. Además, la Agencia ha seguido impulsando la elaboración de códigos de conducta, un procedimiento para resolver de forma más ágil los conflictos que puedan surgir en materia de protección de datos.

Esta Memoria también es el reflejo de que hemos lanzado numerosas iniciativas para proteger a los más vulnerables en Internet, sobre todo en el caso de mujeres y menores. Estamos asistiendo con frecuencia a la publicación en la Red de datos sensibles que afectan, sobre todo, a estos grupos. En 2022 la Agencia realizó a través de su Canal prioritario 51 intervenciones de urgencia para retirar información, imágenes, vídeos o audios publicados sin permiso en Internet y de contenido sensible –sexual o violento–. Las Administraciones educativas tienen establecido por ley la obligatoriedad de enseñar en las aulas un uso de las tecnologías compatible con los derechos fundamentales y, en particular, con el respeto a la intimidad y la protección de datos. Pero la Agencia, en todo caso, no puede permanecer impasible cuando proliferan conductas que implican la difusión de datos personales sin consentimiento y cuyas consecuencias pueden ser devastadoras para la vida de las personas. Tratando de ir a uno de los orígenes de estas conductas, los expertos señalan que el acceso de menores de edad a contenidos online inapropiados y para adultos, en especial a la pornografía, genera importantes desórdenes en la concepción de las relaciones de sexualidad y del rol de la mujer, lo que se traslada también al mundo online. A este respecto, además de impulsar un grupo de trabajo para la verificación de la edad para acceder a esos contenidos, aplicable no sólo a los de carácter pornográfico sino también de violencia explícita, se han finalizado procedimientos sancionadores para proteger a los menores en su acceso online a contenidos para adultos. En el caso de las webs dedicadas a la pornografía titularidad de las empresas sancionadas, existía un riesgo de que los menores de edad accedieran directamente y sin limitaciones a los contenidos.

Los riesgos a los que se enfrentan los menores han de ser considerados por los responsables de los tratamientos, y no sólo por aquellos que dirigen servicios directa y específicamente a los niños sino por todos aquellos que realizan tratamientos de datos personales dirigidos a otros colectivos en los que los menores puedan interactuar o intervenir y poner en riesgo su integridad física o psicológica.

En el plano de concienciación, hay que destacar como una de las principales iniciativas de la Agencia en el año 2022 el lanzamiento de la campaña Más que un móvil junto a UNICEF España, dirigida a ofrecer a las familias las claves que deben tener en cuenta antes de entregar a sus hijos e hijas un teléfono móvil. La campaña ha contado con la colaboración de diversas entidades públicas y privadas, que la han difundido a través de sus respectivos canales

para que todas las familias tengan acceso a unos consejos básicos sobre cómo pueden preparar a sus hijos e hijas para el acceso a la tecnología. Esa campaña, que incluye el decálogo *'La guía que no viene con el móvil'*, recoge pautas y recomendaciones para fomentar el diálogo en las familias, transmitiendo valores e información suficiente para garantizar tanto un uso responsable del teléfono móvil como los derechos de los niños y niñas también en el entorno digital. En este sentido, me siento en la obligación de agradecer a todos los colaboradores la difusión desinteresada que han realizado de la campaña, que ha conseguido más de 290 millones de impactos en 2022 y que se ha convertido en la acción de mayor repercusión en la historia de la Agencia. Como avance, en 2023 ya estamos trabajando con otros organismos, entidades, instituciones y asociaciones para seguir promoviendo pautas y recomendaciones para que las familias participen activamente en la educación digital de sus hijos e hijas.

Además de la firme apuesta por la concienciación en varios planos, la tendencia creciente del número de reclamaciones presentadas ante la Agencia (15.128) también es un reflejo de la preocupación de la ciudadanía por el uso de sus datos personales y la necesidad de control sobre los mismos. Las siguientes páginas reflejan ese ascenso, consolidando una tendencia creciente que supone un aumento del 9% respecto al año 2021 y un 47% respecto del año 2020. Por segundo año consecutivo, el número de reclamaciones recibidas ante esta Agencia ha sido el mayor de su historia. Ello no parece transitorio o circunstancial, lo está suponiendo nuevos retos para esta Agencia. En relación con ello, es obligatorio hacer referencia a la dedicación y el esfuerzo de todos los empleados de la Agencia, un equipo profesional, cohesionado y proactivo que ha seguido trabajando para reducir los tiempos medios de resolución a la vez que ha puesto en marcha acciones de difusión, concienciación y cooperación imprescindibles, tanto dentro como fuera de nuestras fronteras. Sin el buen hacer de todos ellos, los resultados que se recogen en las siguientes páginas no hubieran sido posibles.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

Índice

Memoria 2022

Índice

Memoria 2022

Índice

Anexo. La agencia en cifras

1. Principales hitos de 2022

Nos encontramos en una sociedad digital en la que se intercambian grandes volúmenes de información que es analizada y utilizada para múltiples fines con tecnologías cada vez más avanzadas y a bajo coste.

En ella se ofrecen nuevas posibilidades de relación, gestión del ocio y oportunidades de negocio pero con nuevos riesgos para los ciudadanos.

Y todo ello en el marco de un proceso de concentración de los prestadores de servicios de internet cuyo modelo de negocio está basado en muchas ocasiones en la monetización de la información personal de los usuarios. Lo que lleva a muchas personas a ofrecer sus datos personales a cambio de servicios digitales.

En este entorno la Agencia Española de Protección de Datos tiene la tarea urgente de restablecer la confianza de los ciudadanos sobre el control de sus datos sin que el precio a pagar por la innovación lleve consigo una renuncia a sus derechos.

En la tarea de recuperar la confianza de los ciudadanos la Agencia debe asumir el reto de impulsar de forma dinámica medidas innovadoras que contribuyan a la consecución de ese objetivo de forma holística, es decir, omnicomprensiva de las necesidades que se plantean a todos los agentes implicados: ciudadanos, colectivos vulnerables incluyendo medidas urgentes para evitar la viralidad de videos con imágenes de violencia grave de género o de menores; responsables del tratamiento de datos en el entorno privado y en el de las Administraciones Públicas y encargados del tratamiento.

Medidas que deben ir acompañadas de actuaciones proactivas en relación con las instituciones con competencias el ámbito legislativo de forma que las innovadoras regulaciones que se están desarrollando en el entorno digital sean respetuosas con la garantía de los derechos fundamentales de los ciudadanos.

Y ejerciendo sus poderes de supervisión respecto de los desarrolladores y aplicadores de nuevas tecnologías, en particular de tecnologías disruptivas, de forma que contribuyan positivamente al desarrollo social y eviten sesgos y situaciones de discriminación.

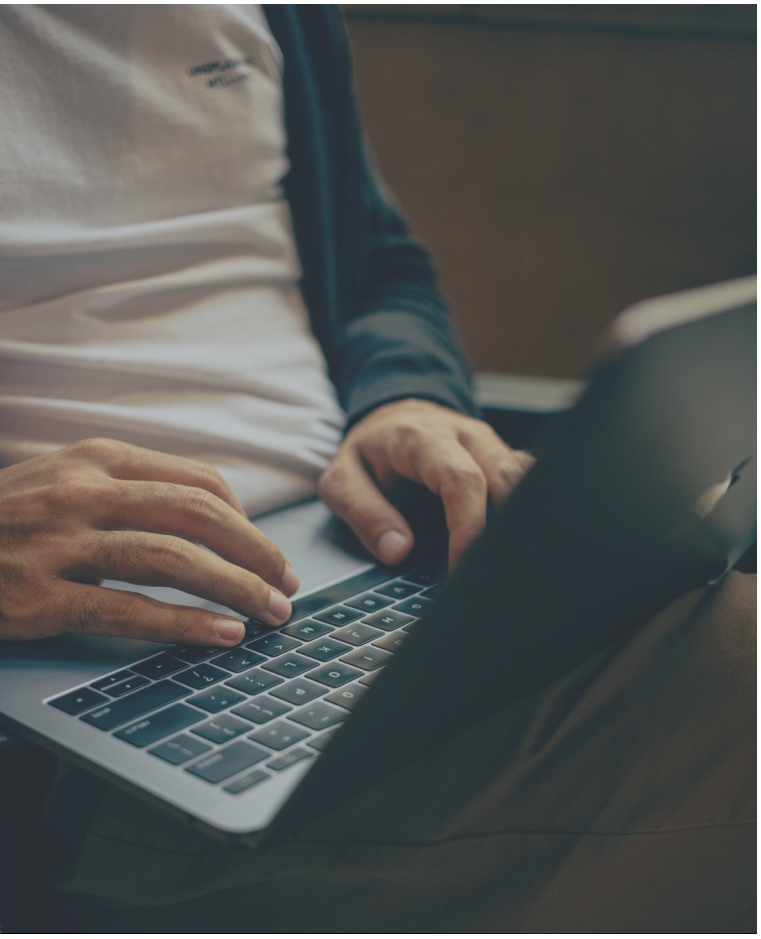
Las medidas proactivas deben incluir de manera destacada la información que se facilita a los ciudadanos sobre las garantías que les protegen y los derechos de los que son titulares, la difusión de orientaciones y guías para facilitar el cumplimiento de las normas, especialmente para las pymes y las startups innovadoras, y el impulso de procedimientos de mediación que permitan dar respuesta con rapidez y eficacia a las reclamaciones de los ciudadanos.

El desarrollo de las tecnologías digitales ha hecho que los datos personales sean considerados el elemento fundamental en la transformación tecnológica, económica y social, en el convencimiento de que el acceso a una cantidad creciente de información y su utilización intensiva son requisitos indispensables para el desarrollo de la economía digital.

La Comisión Europea, en su presentación de su Estrategia Europea de Datos utiliza cifras y proyecciones que ilustran claramente esta evolución. Por ejemplo, la “economía del dato” tenía un valor estimado de 300 mil millones de euros en 2018, mientras que se espera que esa cifra alcance los 829 mil millones en 2025. En el mismo periodo se produciría un incremento del 530% en el volumen global de datos, pasándose de 33 a 175 zetabytes.

Con ese objetivo, se han presentado en la Unión Europea una serie de **propuestas legislativas** que buscan facilitar un mejor acceso y un mayor uso de los datos, personales y no personales, por parte de entidades públicas y privadas, así como apoyar y regular el uso de tecnologías como la inteligencia artificial.

Se trata de propuestas como la Ley de Gobernanza de Datos o el Reglamento de Inteligencia Artificial que viene a plantear la necesidad de establecer un Comité Europeo de Inteligencia Artificial para contribuir a la cooperación efectiva de las propias autoridades nacionales de supervisión que deberán ser designadas por cada Estado miembro con el fin de garantizar la aplicación y ejecución del Reglamento de Inteligencia Artificial de manera objetiva e imparcial en el ejercicio de sus funciones de vigilancia del mercado.



También hay normas ya adoptadas que comparten estos objetivos, como el Reglamento de Datos No Personales o la Directiva de Datos Abiertos y propuestas, como son los Reglamentos sobre Mercados Digitales y sobre Servicios Digitales que buscan regular la actuación de las plataformas online a través de las que tiene lugar una parte sustancial de los tratamientos de datos actuales.

Las autoridades de protección de datos hemos reiterado que es plenamente legítimo promover una mayor disponibilidad y accesibilidad a los datos para usos que contribuyan a ofrecer a los ciudadanos, individual y colectivamente, mejores productos y servicios.

Pero consideramos que la generalización e intensificación del uso de los datos personales debe hacerse desde el pleno respeto a los derechos de las personas y, en particular, pero no solo, a su derecho a la protección de datos tal y como lo entendemos en el entorno europeo.

Y es ahí donde surge la preocupación de las autoridades de protección de datos.

Todas las normas que se han citado parten de reconocer la necesidad de respetar el modelo de protección de datos diseñado por el Reglamento General de Protección de Datos (RGPD) y subrayan la importancia de hacerlo, entre otras cosas, para conseguir la confianza de los ciudadanos.

Sin embargo, el modo en que esas normas están concebidas hace que surjan problemas en su consistencia con el Reglamento que aseguran respetar.

Estas normas se elaboran desde la perspectiva del sector o tecnología que pretenden regular y, lógicamente, su principal objetivo es lograr la eficacia y eficiencia en su funcionamiento.

Eso hace que se produzcan inconsistencias que pueden afectar significativamente al modo en que se garantiza la protección de los datos personales.
En los dictámenes elaborados por el Comité Europeo de Protección de Datos y por el Supervisor Europeo de Protección de Datos, algunos de ellos de forma conjunta, se han identificado tres grandes grupos de esta falta de alineación entre estas normas y la normativa de protección de datos.

Uno incluye los conceptos utilizados, otro las habilitaciones y obligaciones que se establecen para los actores en cada caso y un tercero la gobernanza de los diferentes sistemas, incluido el esquema sancionador.

Cuando la terminología empleada no coincide con la que utiliza el RGPD o coincidiendo y se da a los conceptos diferente contenido, resulta difícil determinar cómo aplicar la normativa de protección de datos en cada contexto.

De igual modo, varias de estas normas contemplan tratamientos de una forma que no está en línea con las previsiones sobre bases jurídicas en el RGPD.

Respecto al sistema de gobernanza, en muchas de estas normas, como sucede con la Ley de Gobernanza de Datos o con el Reglamento de Inteligencia Artificial, se establecen unos mecanismos de supervisión que incluyen sus propias autoridades, dotadas de funciones que pueden ir desde la autorización de determinadas actividades a la imposición de sanciones.

El problema es que no está bien definida cuál ha de ser la articulación de esos sistemas de gobernanza con el sistema existente en el ámbito de protección de datos.

En algunos casos las autoridades de protección de datos tienen un papel secundario en esos sistemas, pese a que el uso de datos personales forma parte esencial de los usos o intercambios que se regulan.

Nos encontramos, en suma, en un momento crucial. Es indudable que avanzamos a gran velocidad a un escenario de usos masivos y generalizados de la información personal y que es preciso afrontar esa realidad, aceptando que no se puede, y en muchos casos, no se debe, detener ese avance. Pero incorporando reglas que establezcan garantías, por lo que hay que seguir trabajando para mejorar las garantías que permitan que la mayor disponibilidad y utilización de los datos no reduzcan por vías alternativas el nivel de protección de los datos personales que hemos conseguido.

Reiterando, frente a quienes mantienen de forma expresa o subyacente lo contrario, que el derecho a la protección de datos no es un obstáculo para la innovación y el beneficio de la sociedad.

Lo que exige articular procedimientos efectivos de cooperación entre las autoridades de protección de datos personales con las autoridades de gobernanza previstas en el citado bloque normativo.

Adicionalmente, dados los años transcurridos desde la aplicación efectiva del Reglamento General de Protección de Datos resulta conveniente evaluar la situación real de aplicación de elementos críticos del principio de responsabilidad proactiva en relación con el marco normativo que incida en el tratamiento de datos personales mediante la elaboración de disposiciones de carácter general que afecten al derecho fundamental a la Protección de Datos.

Así como en la aplicación práctica de dicho principio en elementos esenciales del modelo de cumplimiento como son a la figura de los delegados de Protección de Datos, los procesos de análisis de riesgos a través de evaluaciones de impacto en la Protección de Datos (EIPD) y la notificación de brechas de seguridad, que se describen a continuación y cuyo detalle se amplía en distintos apartados de esta memoria.

Respecto de los retos en el ámbito normativo, se constata una omisión relevante que están poniendo de manifiesto los preceptivos informes de la Agencia sobre los anteproyectos de disposiciones de carácter general que afectan al tratamiento de datos personales.

Se trata de la exigencia de que en la Memoria de Análisis de Impacto Normativo (MAIN) se incluya la documentación acreditativa de la EIPD, así como un artículo o disposición específica que contemple la incidencia de los tratamientos regulados en la norma respecto de la normativa de protección de datos personales (bases jurídicas, finalidades de los tratamientos, posición jurídica de los intervinientes, etc.) conforme a las previsiones del Reglamento General de Protección de Datos la LOPDGDD, así como a las recogidas en la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional relativas a la inclusión de un artículo o una disposición que contemplara la incidencia en la protección de datos personales del contenido de los proyectos de disposiciones de carácter general.

A lo que se añade una segunda omisión relevante como es la ausencia del criterio de los delegados de protección de datos sobre las mismas.

El segundo de los retos está relacionado con él cumplimiento del principio de responsabilidad proactiva del Reglamento en dos de sus principales manifestaciones: la realización de la EIPD y el desarrollo de las funciones de los DPD.

Respecto de las EIPD, se aprecia con carácter general un intento de cumplimiento meramente formal sin dar respuesta al enfoque de riesgos sobre los derechos de las personas.

Las consultas presentadas a la Agencia en este ámbito se han limitado a un análisis de riesgo de cumplimiento normativo y no a una gestión de riesgos. Asimismo, se aprecia una falta de participación de los delegados de protección de datos, tanto en el asesoramiento como en la supervisión de las EIPD.

Adicionalmente, la experiencia que nos han proporcionado estos más de 4 años de aplicación del RGPD han puesto de manifiesto ciertas carencias y deficiencias en la figura del DPD, en las que tiene mucho que ver la actuación y disposición de los responsables y encargados del tratamiento.

En este sentido hay que destacar la condición que tanto el RGPD como la LOPDPGDD atribuyen a los DPD como elementos clave en el sistema de cumplimiento y garantía del derecho a la protección de datos. **La experiencia de estos años de funcionamiento de los DPD y la preocupación por un buen ejercicio de sus funciones** ha determinado que la Agencia se interese por su designación y situación, mediante la elaboración de un cuestionario y su distribución por el momento en el ámbito de las Administraciones Públicas. Las respuestas recibidas hasta la fecha que permiten obtener conclusiones, fundamentalmente las de la AGE, ponen de manifiesto una serie de deficiencias en sus nombramientos, vinculadas a la falta de la cualificación, y a la carencia de respaldo y apoyo de los responsables para que puedan ejercer con independencia sus funciones.

Sintéticamente las respuestas recibidas a la encuesta señalan que la designación no siempre obedece a los requisitos de cualificación, pues se aprecia un déficit en la formación de los DP y que un alto porcentaje, lo es a tiempo parcial, lo que en organismos con varios centros directivos y multitud de usuarios, resultaría insuficiente y demandaría más medios para desarrollar su labor.

En cuanto a la participación de los DPD en los asuntos relativos a la protección de datos también se muestran carencias, respecto de dos medidas de cumplimiento muy relevantes, como son las evaluaciones de impacto y la notificación de brechas de seguridad.

Otro aspecto de la situación de los DPD es el relativo a la ausencia o débil apoyo y respaldo que reciben de los responsables, de los que se necesitaría una mayor implicación, pues su aportación constituye un importante valor para el desarrollo de las actividades de su competencia.

El último de los retos destacado de esta memoria es el relacionado con el modelo de supervisión.

La proliferación de las nuevas tecnologías ha propiciado nuevas amenazas, en parte causadas por la velocidad de difusión de información e imágenes, la facilidad de acceso a las mismas a través de los motores de búsqueda y las dificultades para eliminarlas de internet. La violencia de género ha pasado de ser física o psicológica a incluir el ciberacoso y la vulneración de la privacidad de las víctimas con acciones como la grabación y distribución de imágenes con contenido sensible en las redes sociales. Por tanto, las nuevas tecnologías se emplean en algunos casos para controlar, acosar, humillar, extorsionar o atemorizar. Aunque todo ciudadano puede ser una víctima, los menores de edad y las mujeres son el principal blanco de estas conductas.

Con el fin de hacer frente a estos riesgos el Canal Prioritario de la AEPD para comunicar la difusión ilícita de contenido sensible y solicitar su retirada pretende ofrecer una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento.

En cuanto a las iniciativas, desarrollos y cumplimiento de las medidas de responsabilidad social corporativa de la Agencia Española de Protección de Datos debe indicarse que por su amplitud y relevancia se describen en una memoria específica.

2. Desafíos para la privacidad

De las iniciativas del paquete digital de la Comisión Europea antes citado, si hubiera que destacar algún tratamiento en dónde será más crítica dicha agenda, lo encontramos en aquellos que se están desarrollando en torno a componentes de IA. El uso de la IA por parte de los poderes públicos y las empresas privadas constituye uno de los principales hitos del siglo XXI.

En el Reglamento de Inteligencia Artificial, se permiten, o no se prohíben con la extensión o contundencia apropiadas, determinados usos que implican tratamientos de datos personales y que pueden afectar a los derechos de los ciudadanos y dar lugar a situaciones de discriminación.

Un ejemplo en ese sentido es el de los sistemas de IA que el Reglamento prohíbe. La prohibición alcanza, entre otros, a los "sistemas de IA que aprovechen alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra."

Tal y como está definido el ámbito de la prohibición, parece que es posible emplear sistemas de IA que aprovechen las vulnerabilidades de personas que no pertenezcan a esos colectivos. O que se pueden emplear esos sistemas siempre que la alteración en el comportamiento no sea "sustancial" o que no se causen perjuicios físicos o psicológicos.

Sin embargo, hay que tener en cuenta que tanto el RGPD, como el nuevo paquete normativo que la Comisión Europea ha planteado en el marco de la Estrategia Europea de Datos, establecen que la tecnología ha de implementarse de forma que el preservar el marco de derechos y libertades de los ciudadanos sea el motor que permita aprovechar las oportunidades que puede aportar una economía digital en beneficio de nuestra sociedad.

En nuestro país ya se ha planteado la creación de la Agencia Estatal de Supervisión de Inteligencia Artificial, por lo que la AEPD, dicha Agencia, y todas las agencias y autoridades implicadas en la estrategia digital han de colaborar, estrechamente, de forma eficiente y desde el diseño de dicha estrategia para conseguir dicho objetivo.

La digitalización y las tecnologías digitales permiten el tratamiento de datos a una escala desconocida hasta ahora, con la posibilidad de conseguir propósitos que eran inviables hace una década, y que a la vez encierran un gran poder de transformación de los modelos económicos y sociales.

Uno de los escenarios que se plantean para ello son los Espacios de Datos.

En los **Espacios de Datos** se plantea un modelo de tratamiento de gran complejidad organizativa y tecnológica, así como el escalado en la diversidad de categorías de datos procesadas, número de sujetos afectados, ámbitos involucrados, intervinientes y otros. Todas estas circunstancias conllevan una capacidad de obtener grandes resultados, pero también el aumento del riesgo de un impacto indeseado sobre los individuos y la sociedad en múltiples aspectos, en particular, con relación a los derechos y libertades fundamentales.

Cuando en el Espacio de Datos se realicen tratamientos de datos personales, el cumplimiento del principio de responsabilidad proactiva exige la aplicación de medidas técnicas y organizativas apropiada, a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento General de Protección de Datos, teniendo

en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas (art.24 RGPD).

La Agencia Española de Protección de Datos está colaborando con las iniciativas de la Administración General del Estado sobre espacios de datos y analizando sus implicaciones con el fin de poder elaborar unas orientaciones que faciliten su adecuación a la normativa de protección de datos personales.

2.1. El mundo digital

Una de las principales preocupaciones del actual entorno digital es el relacionado con el acceso a los dispositivos móviles por parte de los menores, al periodo temporal en que los utilizan y a los servicios de internet a los que acceden.

Los datos a los que se hace referencia más adelante en el apartado 3 muestran un uso intensivo y prácticamente universal de Internet que implica riesgos cuando éste no se realiza con responsabilidad, en particular por parte de colectivos vulnerables. Lo que hace cada vez más necesaria la presencia de medidas preventivas que permitan obtener el máximo provecho de las oportunidades que ofrece la tecnología sin exponerse a los riesgos que puede presentar cuando se utiliza de manera inapropiada.

Con el fin de dar respuesta a esta situación, debe destacarse como una de las principales iniciativas de la Agencia en el año 2022, la campaña “Más que un móvil” realizada conjuntamente con UNICEF España y con la colaboración de diversas entidades públicas y privadas en la que se facilitan unos consejos básicos a las familias sobre los aspectos a tener en cuenta antes de facilitar un teléfono móvil a los menores.

A su vez, la evolución de las tecnologías digitales, como la inteligencia artificial, disponible y aplicable por el sector público y el privado, el internet de las cosas, e iniciativas como la de los mercados y servicios digitales, para la reutilización de información y datos personales, o la creación de

espacios comunes de datos en diversos sectores, entre ellos el de la salud, afecta de manera directa a la privacidad de las personas y a sus derechos y libertades, lo que constituye un desafío para el derecho fundamental a la protección de datos que exige que se sitúe al ser humano en el centro del desarrollo tecnológico.

2.2. Jurídicos

2.2.1 Consultas

Durante el ejercicio 2022 se observa un cambio de tendencia en las consultas que se atienden en el Gabinete Jurídico tanto en el aspecto cualitativo como cuantitativo, y que si bien puede obedecer a distintas causas, hay que destacar la aprobación de la Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, que entró en vigor el 6 de noviembre del año 2021 pero que ha tenido una gran incidencia en el año 2022, al definir con claridad cuáles son las funciones consultivas que debe desarrollar la AEPD, de conformidad con el RGPD y la LOPDGDD y su Estatuto.

Las funciones consultivas de la AEPD deben adaptarse al nuevo esquema jurídico creado por el RGPD, que no contempla el asesoramiento individualizado a responsables o encargados por la autoridad de control ni la consulta particular a demanda de los responsables. Se reitera la implicación de los responsables y encargados, a la hora de analizar los riesgos del tratamiento de datos personales y las garantías que permitan mitigarlos y la necesaria intervención del Delegado de Protección de Datos.

De acuerdo con la referida Instrucción, las autoridades de control tienen un carácter marcadamente de supervisión y no se encuentran entre sus funciones, listadas en el artículo 57 del RGPD, las de asesorar o resolver las consultas de los responsables o encargados del tratamiento, porque son ellos mismos, asistidos por sus DPD, o abogados o consultores, quienes han de determinar los tratamientos de datos que implique el ejercicio de su actividad, evaluar los riesgos que su suponen para los derechos y libertades de los afectados e implantar las medidas necesarias para evitarlos o reducirlos. Así, el asesoramiento jurídico personalizado e individualizado a los responsables y los encargados del tratamiento sólo corresponde a los abogados o consultores y a los delegados de protección de datos.

En consecuencia, el Gabinete Jurídico ha centrado principalmente su actividad en la emisión de informes preceptivos sobre disposiciones legales y reglamentarias, así como de aquellos otros a asuntos de carácter jurídico en los que debiera consultarse, preceptivamente, a la AEPD, en virtud de disposiciones legales o reglamentarias. También de conformidad con la Instrucción, ha emitido informes sobre consultas presentadas por los Delegados de Protección de Datos que, acompañaban el respectivo informe con las valoraciones y conclusiones a las que llegaran, y que no pudieran resolverse con criterios ya informados anteriormente o que tratasen de cuestiones novedosas y siempre que tuvieran un alcance general y cuya resolución contribuyera a la seguridad jurídica, tanto de obligados como de la ciudadanía en tanto titular del derecho fundamental.

Teniendo en cuenta el marco de actuación que se acaba de indicar procede destacar los siguientes informes.

Los Informes 1/2020 y 22/2022 en los que la Comisión Nacional de los Mercados y la Competencia (CNMC) plantea la adecuación al marco jurídico vigente de protección de datos, de las solicitudes que frecuentemente recibe del Centro de Investigaciones Sociológicas (CIS) para que le sean suministrados los números telefónicos de abonados para la realización de distintos estudios y encuestas.

Estos informes son relevantes pues en ellos se establece la necesidad de abordar una modificación legislativa que finalmente se produjo, lo que les hace acreedores de la correspondiente cita en la presente memoria anual.

En el primero de ellos se solicita el criterio de la AEPD, tras la modificación del artículo 49.1 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, sobre si la comunicación por parte de la CNMC al CIS de los datos relativos a los números de teléfono de los abonados facilitados por los operadores a través del SGDA (Sistema de Gestión de Datos de Abonados), que no hayan dado su consentimiento para figurar en guías de abonados o en servicios de consulta sobre números de abonados, resulta conforme a la normativa de protección de datos personales para las finalidades manifestadas por el CIS.

En el informe se cita el criterio mantenido en otros sobre la adopción de garantías adicionales por parte del responsable del tratamiento **(Informes 41/2020, 78/2020 y 98/2020)** y recuerda de nuevo la necesidad de que se impulse la correspondiente modificación legislativa que garantice la seguridad jurídica y la adecuación de los correspondientes tratamientos de datos personales al RGPD y a la doctrina del Tribunal Constitucional, mediante el establecimiento de las garantías específicas que se estimen adecuadas. Dicha observación se reiteró en el **Informe 46/2021, referente al Anteproyecto de Ley General de Telecomunicaciones.**

Pues bien, la modificación legislativa aconteció con la modificación del artículo 49.1 LGT que motiva la consulta, sin que pudiera informarse por la AEPD la misma ya que esta se produjo en el trámite parlamentario.

En consecuencia, el informe tras analizar los supuestos legitimadores del tratamiento propuesto, y las exigencias legales y jurisprudenciales sobre los requisitos que tiene que tener la disposición de carácter general que afecte al derecho fundamental, concluye que el citado artículo 49.1 LGT ampara, con carácter general y por la existencia de una obligación legal, la comunicación de los datos de los abonados a los servicios estadísticos oficiales, pero sin que se puedan incluir en la comunicación los datos de aquellos abonados que hayan ejercido su derecho a no figurar en las guías, ya que ello requeriría que el legislador lo hubiera incluido expresamente justificando adecuadamente dicha inclusión en la necesidad de adecuar los datos facilitados a las muestras previamente identificadas.

Como puede observarse propone de nuevo la correspondiente modificación Legislativa.

Por su parte, el segundo **informe citado 22/2022**, aborda la comunicación por parte de la CNMC al CIS de una muestra de 312.000 números de teléfono aleatorios y anónimos (distribuidos provincialmente de forma aleatoria), para la realización de cada una de las tres oleadas del Barómetro Sanitario.

Se pone de manifiesto que se trata de una encuesta de cumplimentación voluntaria, ya que, al implicar el tratamiento de categorías especiales de datos, el artículo 5 de la Ley 39/1995, de 19 de diciembre, de Organización del Centro de Investigaciones Sociológicas recoge el principio de voluntariedad de las respuestas.

Por consiguiente, se indica que la comunicación de los números de teléfono al CIS, incluyendo los de aquellos abonados que no hayan dado su consentimiento para figurar en guías de abonados o en servicios de consulta sobre números de abonados, únicamente procederá, con carácter excepcional, siempre y cuando las circunstancias derivadas de la pandemia así lo exijan en el momento de realizar cada una de las oleadas, lo que se deberá justificar oportuna y motivadamente por el CIS.

El informe finaliza proponiendo determinadas garantías especificas dirigidas a conciliar la efectividad del derecho a la protección de datos y el derecho a no figurar en guías de abonados con el ejercicio de las funciones públicas legalmente atribuidas al CIS y que se concretan en las siguientes:

- Únicamente se facilitará el número de teléfono y la provincia a la que corresponde, sin facilitar ningún otro dato que permita la identificación directa de los abonados.
- Realizada la llamada, la obtención de otros datos de carácter personal quedará condicionada a la previa prestación del consentimiento por el afectado.
- Los números de teléfono de aquellas personas que no hayan prestado su consentimiento serán inmediatamente suprimidos. Los de las personas que hayan participado en la encuesta deberán suprimirse desde el momento en que no sean necesarios y, en todo caso, en el plazo máximo de un mes desde la realización de la encuesta.
- Los números de teléfono facilitados únicamente podrán utilizarse para la realización de la encuesta para la que han sido solicitados, no pudiendo utilizarse para la realización de otras encuestas distintas ni para ningún otro fin diferente.

Como se ha indicado antes, estos informes han tenido como consecuencia el cambio legislativo que demandaban, habiéndose materializado en la modificación del artículo 72.2 e) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que recoge los supuestos y garantías para poder llevar a cabo este tipo de tratamientos.

En segundo lugar, procede citar los informes emitidos por el Gabinete Jurídico en relación con la elaboración y aprobación de distintos Códigos de Conducta previstos en el artículo 40 del RGPD.

En este ámbito se incluyen el **Informe 4/2022 relativo al Código de Conducta Regulador del Tratamiento de datos personales en el ámbito de los Ensayos Clínicos y otras investigaciones clínicas y de la Farmacovigilancia"** promovido por Asociación Nacional Empresarial de la Industria Farmacéutica (Farmaindustria), el **Informe 32/2022 relativo al Código de Conducta Regulador del Tratamiento de Datos Personales en los Sistemas Comunes del Sector Asegurador**, promovido por la Unión Española de Entidades Aseguradoras (Unespa), y finalmente, el **Informe 97/2022 relativo al "Código de Conducta de tratamiento de datos en la actividad publicitaria"** promovido por la Asociación para la Autorregulación de la Comunicación Comercial (Autocontrol).

Adicionalmente procede hacer referencia al **Informe 98/2022 que aborda el tratamiento de datos biométricos**. En él, se analiza la adecuación a la normativa vigente del acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia, que establece medidas a cumplir por los clubes deportivos consistentes en la instalación de sistemas biométricos para el control de accesos a las gradas de animación que permita la identificación unívoca de los aficionados, al amparo del artículo 13.1 de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, que faculta a dicha Comisión, para decidir la implantación de medidas adicionales de seguridad para el conjunto de competiciones o espectáculos deportivos calificados de alto riesgo, o para recintos que hayan sido objeto de sanciones de clausura , incluida en particular, la de promover sistemas de verificación de la identidad de las personas que traten de acceder a los recintos deportivos.

El informe señala que teniendo en cuenta que la consulta se refiere a un supuesto de tratamiento de datos biométricos con la finalidad de verificar identificar, de forma unívoca, a los aficionados que accedan a las gradas de animación, dicha circunstancia implica por si sola el tratamiento de categorías especiales de datos sujeto a la regla general de prohibición de los mismos (art. 9.1. RGPD).

En consecuencia, realiza el análisis de los presupuestos necesarios para poder aplicar la excepción a la prohibición general del tratamiento de categorías especiales de datos prevista en el apartado g) del articulo 9.2 RGPD, referida a los requisitos legales de los que debe ser acreedora la norma que establezca la injerencia en el derecho, en cuanto a la determinación del interés público esencial, los presupuestos necesarios y las garantías específicas. (STC 76/2019 de 19 de mayo) destacando que (…) el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos. Además, la norma deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero (…) .El informe señala que el artículo 13.1 de la Ley 19/2007, de 11 de julio hace referencia a sistemas de verificación de la identidad, pero no contempla la posibilidad de que dichos sistemas puedan implicar tratamientos de datos biométricos, ni establece las garantías pertinentes y adecuadas para la protección del derecho fundamental a la protección de datos personales. Dicha posibilidad tampoco aparece prevista en el artículo 15.3 del Real Decreto 203/2010, de 26 de febrero, aunque debe adelantarse que dicha norma carecería, tal y como se viene exponiendo, del rango legal adecuado para proceder a la regulación del tratamiento de categorías especiales de datos personales. Y tampoco el acuerdo de la Comisión podría suplir las carencias normativas apuntadas.

Concluyendo que la adopción de un acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia, en el ámbito de sus competencias, estableciendo medidas para el cumplimiento de los clubes consistentes en la instalación de sistemas biométricos para el control de todos los accesos a las gradas de animación que permita la identificación unívoca de los aficionados que accedan a dichas gradas, no es conforme con la normativa reguladora de protección de datos.

Siguiendo con los tratamientos de categorías especiales de datos, otro aspecto sobre el que el Gabinete Jurídico ha manifestado su criterio es el relativo al tratamiento del dato relativo a la discapacidad en procedimientos de concurrencia competitiva por parte de las administraciones públicas.

En el **Informe 2/2022** **se aborda cómo debe tratarse el dato relativo a la condición de discapacitado para conjugar el derecho a la protección de datos con las obligaciones de transparencia y publicidad en los procesos selectivos**. Se plantea si es conforme a la normativa de protección de datos la publicación en un proceso selectivo de acceso al empleo público, de la lista de admitidos y excluidos con la indicación del turno por el que se participe, en concreto, por el turno de discapacidad. Se abre el debate si tal condición -la de discapacidad- debería ser privada y por tanto utilizarse otros medios de identificación como el DNI o algún código alfanumérico.

En el informe se analiza en primer lugar, la base jurídica que legitima el tratamiento de este tipo de datos en los procesos selectivos, para lo que se recuerdan los criterios que establece el Informe 86/2020 donde se excluye expresamente el consentimiento por carecer de libertad a la hora de su prestación y se afirma que el tratamiento del dato relativo a la condición de discapacidad que, con carácter general realizan las administraciones públicas en la provisión de empleo público, resulta conforme a lo dispuesto en el artículo 9.2 b) y articulo 6.1 b), c) y e) del RGPD.

En segundo término, se aborda cómo se ha de conjugar el principio de publicidad y transparencia de los procesos selectivos con el derecho a la protección de datos, con cita de jurisprudencia como la del Tribunal Supremo en sentencia núm. 2487/2016 de 22 noviembre, o la de la Audiencia Nacional en sentencia de 26 de abril de 2012 recaída en el recurso 215/2010 indicando que es necesario hacer un ejercicio de ponderación y que la garantía de publicidad y transparencia en un procedimiento de concurrencia competitiva ha de prevalecer, teniendo en cuenta el caso concreto, sobre el derecho a la protección de datos, pero observando los límites del principio de minimización.

Y para la aplicación de dicho principio y de la proporcionalidad de la publicación, se analizan multitud de resoluciones tanto de la AEPD como de otros organismos con competencia en la materia como el Consejo de Transparencia de Aragón, la Agencia Vasca de Protección de Datos, o la Autoridad Catalana de Protección de Datos, recordando las obligaciones de los responsables del tratamiento en relación con la aplicación del artículo 25 del RGPD referido a la “Protección de Datos desde el diseño y por defecto” , el Considerando 78 y el propio artículo 28 de la LOPDGDD en relación con la aplicación de medidas en relación al riesgo que pueden tener determinados tratamientos, como aquellos supuestos que puedan generar situaciones de discriminación, o perjuicio moral o social, aquellos en los que se traten categorías especiales de datos o de grupos de afectados en situación de vulnerabilidad y en particular personas con discapacidad, y aquellos que conlleven un tratamiento masivo de datos, como son los procesos selectivos. Finalmente establece las siguientes conclusiones:(…) Las medidas que se analizan y proponen en las conclusiones del presente informen podrían resultar adecuadas y recomendables, incluso para la publicación del listado del turno de acceso libre, teniendo en cuenta los riesgos derivados del estado de la tecnología actual y la exponencial transmisión y publicación de cualquier información que se produce a través de internet. En consecuencia, se proponen medidas aplicables con carácter general a la publicación de datos

personales en los procesos selectivos, aplicables a ambos turnos de participación, cuya concreción e implementación corresponde en todo caso al responsable del tratamiento en cumplimiento del principio de responsabilidad activa, y que con independencia de las que considere oportunas, deberá tener en cuenta la especial protección que requiere el dato de discapacidad.

(…) se proponen, como adecuadas al principio de minimización, confidencialidad y protección de datos desde el diseño y por defecto en relación con el principio de publicidad y transparencia que ha de informar los procesos selectivos de acceso a la función pública, medidas diferenciando el acceso a las publicaciones a través de internet del acceso a las publicaciones en tablones de anuncios físicos en las sedes correspondientes.

Respecto del acceso a través de internet, establecer el acceso restringido con usuario y contraseña a los participantes en el proceso selectivo, entendidos como tales aquellos que hayan formalizado la correspondiente instancia, o mediante el uso del DNI electrónico o certificado digital. Recuérdese que el articulo 25.2 RGPD indica que tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. (…). Añadiendo que los interesados podrán acceder a los listados de admitidos y excluidos, de aprobados de los ejercicios en los que se constituyan las pruebas del proceso selectivo y aprobados finales, con la calificación correspondiente. El acceso podrá realizarse de modo indistinto, es decir, los del turno libre podrán acceder a los listados del turno de discapacitados y viceversa. La razón de ser de esta posibilidad es que en numerosas ocasiones las bases de los procesos selectivos prevén que (…) en el supuesto de que algunas de las personas aspirantes que se haya presentado por el cupo de reserva de personas con discapacidad superase los ejercicios correspondientes, pero no obtuviese plaza y su puntuación fuese superior a la obtenida por otras personas aspirantes del sistema de acceso general, éste será incluido por su orden de puntuación en el sistema de acceso general. (…). Y también que aquellas plazas de este último que no son cubiertas se incorporan o acumulan al turno general. Por lo que resulta obvio la existencia de un interés legítimo en que los participantes de ambos turnos puedan conocer las listas de admitidos y excluidos indistintamente. (…) En cuanto a la información a la que se accede, en los correspondientes listados referenciados en el párrafo anterior, se identificará a cada participante con la asignación un código -que podría ser el mismo que se otorgara con la instancia de participación y que constituye a su vez el nombre de usuario del acceso a la información sobre el proceso selectivo y las iniciales de los nombres y apellidos de cada participante y el DNI en los términos de la Disposición Adicional Séptima de la LOPDGDD. Así se da cumplimiento al principio de minimización no publicando más datos de los necesarios para cumplir la finalidad a la que sirve el tratamiento. En cuanto al plazo durante el que deben estar accesibles dichos listados, de acuerdo con el articulo 5.1 e) RGPD sobre limitación del plazo de conservación, deberán ser accesibles mientras sirvan a la finalidad a la que sirven. Así, por ejemplo, la lista de admitidos y excluidos se deberá eliminar del sitio web en tanto venzan los plazos sobre su impugnación, o las listas sobre la calificación de un ejercicio concreto, mientras no haya precluido el trámite para su impugnación. (…). Finalmente, en cuanto a los nombramientos como empleados públicos de aquellos participantes que hayan superado el proceso selectivo, el articulo 62 EBEP obliga a publicar el nombramiento de los funcionarios de carrera en el diario oficial correspondiente, pero nada dice de la publicación por el turno en el que participaban. Teniendo en cuenta las medidas que se acaban de indicar, nada impide que aquellos participantes que pretendan conocer la identidad completa de otros participantes, con la finalidad de ejercer los derechos que el ordenamiento jurídico les concede, como aquellos derivados de la LPACAP, del EBEP o de las convocatorias en cuestión, puedan acceder a dicha información.(…) Para el resto de las personas, no participantes la publicación del proceso selectivo, la publicación en internet referida al proceso selectivo contendrá aquellos actos o fases del mismo sin indicación alguna sobre datos de carácter personal, incluso los seudonimizados.

En cuanto al acceso a los listados en los espacios físicos donde se encuentren los Tablones de Anuncios de las correspondientes sedes, se aplicarían en cuanto al contenido y plazo de publicación lo indicado hasta ahora, y en cuanto a la accesibilidad al lugar dónde se encuentren los mismos, se deberían adoptar medidas para que no fueran de libre acceso, sino que se justifique la condición de participante en el proceso selectivo.

El informe finaliza poniendo de manifiesto la necesidad de proponer la correspondiente modificación legislativa teniendo en cuenta la ausencia de normas específicas sobre el modo concreto de proceder, la inexistencia en la práctica, de uniformidad de criterios, y las numerosas administraciones y organismos públicos que tienen competencias sobre la ejecución de procesos selectivos al empleo público.

En quinto lugar, procede citar los Informes 28/2022 y 37/2022 cuyo denominador común es que se analiza el tratamiento de datos que supone a los legalmente obligados, el cumplir determinados requerimientos de la autoridad pública. El primero aborda el análisis de los requerimientos del Tribunal de Cuentas a los partidos políticos y el segundo los requerimientos de la Sindicatura de Cuentas de las Islas Baleares a los distintos organismos de la administración autonómica.

En el Informe 28/2022 además se analiza el tratamiento desde la perspectiva de las categorías especiales de datos, habida cuenta que el Tribunal de Cuentas tiene, entre otras, atribuidas las competencias de control y supervisión que se establecen en la Ley sobre Financiación de Partidos Políticos lo que le habilita para conocer información que puede revelar la ideología, al tener que acceder a las fuentes de financiación de los mismos como pueden ser las donaciones o las cuotas de afiliados.

El informe, tras analizar la naturaleza jurídica y el régimen jurídico del Tribunal de Cuentas, tiene como punto de partida que el tratamiento de datos que se deriva del ejercicio de sus competencias y funciones nace de la Constitución y de la ley orgánica, por lo que se daría cumplimiento al principio de licitud recogido en el artículo 5.1 a) del RGPD, al tratarse de un tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) del RGPD. Y respecto del partido político requerido, el tratamiento que se derive del cumplimiento de los requerimientos nace de una obligación legal, por tanto, amparada en el artículo 6.1 c) RGPD.

Para dar cobertura al posible tratamiento de categorías especiales de datos, el informe señala de aplicación el articulo 9.2 g) RGPD, señalando que el Tribunal de Cuentas es una autoridad pública cuyas funciones están previstas constitucionalmente y reguladas en lo que aquí interesa en cuatro leyes, tres de ellas orgánicas y otra ordinaria, resaltando el indudable interés público esencial de sus cometidos que se deriva del texto de la propia Ley Orgánica 8/2007, de 4 de julio, sobre financiación de los partidos políticos.

En cuanto al cumplimiento de otros principios como el de limitación de finalidad y minimización, el informe tras analizar diversa jurisprudencia europea como la STJUE de 24 de febrero de 2022, Asunto C-175-20, o la STJUE de 1 de agosto de 2022 Asunto C184/20, realiza una comparativa con el criterio sostenido hasta la fecha por la AEPD sobre el concepto de “trascendencia tributaria” para legitimar determinados tratamientos de datos, que en el caso analizado estaría referido a la “trascendencia económico, financiera y contable” como elemento esencial de los requerimientos del Tribunal de Cuentas para adecuarlos a los principios de limitación de finalidad y en su caso, minimización.

Indicando que en todo caso dicha trascendencia no le corresponde apreciarla a la AEPD, sino que es la administración requirente la que debe haberla apreciado previamente y en su caso, invocarla y es la entidad requerida la que, a través de las vías legales oportunas, puede recurrir los actos de petición concretos o el resultado final del procedimiento de que se trate por infracción del ordenamiento jurídico vigente, entre el que se encuentra, obviamente, el régimen de protección

de datos. Y en último término será en vía judicial donde se confirme o no dicha trascendencia (tributaria, económico-contable, etc.,) que puede ser directa, indirecta o incluso hipotética, siendo el parámetro que va a servir para determinar si la petición sirve a la finalidad y, en consecuencia, si resulta proporcional.

El informe compara los requerimientos que denuncia el partido político con determinados preceptos que legitiman la actuación del Tribunal de Cuentas observando que, a priori y sin perjuicio del juicio técnico que no le corresponde a la AEPD, son conforme a los principios de limitación de finalidad y minimización.

Finalmente se recuerda el criterio de la AEPD sobre los requerimientos de información que realizan las autoridades públicas en el ejercicio de sus funciones el sentido de que deben ser concretas, motivadas y no suponer una cesión masiva de datos. Y que, en esa motivación, se ha de consignar si la petición sirve a la finalidad del tratamiento en cuestión como recoge el Informe 59/2021 a cuyo tenor: (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley. (…) con lo que la pertinencia y necesidad del tratamiento deberá justificarse adecuada y expresamente por el solicitante de los datos (…)

El **Informe 37/2022** es similar al que se acaba de analizar, siendo el órgano requirente la Sindicatura de Cuentas de las Islas Balears, y la entidad requerida la Oficina de Prevención y Lucha contra la corrupción.

La principal diferencia es que, en este caso, se plantea por la citada Oficina que el requerimiento recibido al referirse a procesos selectivos de provisión de puestos de trabajo en dicho organismo es un aspecto que conlleva tratamiento de datos personales y que queda fuera del control de la actividad económica, contable y financiera que le corresponde a la Sindicatura de Cuentas. Es decir, a juicio del requerido se estaría solicitando información que contiene datos personales para una finalidad que no se corresponde con las funciones que el organismo autonómico de supervisión económico, financiero y contable tiene atribuidas. Por tanto, no se tendría base jurídica de legitimación y, en consecuencia, también se incumplirían los principios de limitación de finalidad y minimización.

En el informe, se analiza la naturaleza y régimen jurídico de la Sindicatura de Cuentas, en relación con la petición de información, indicando que ésta sirve a la finalidad de verificar que el gasto de personal que se deriva de cualquier proceso selectivo es conforme a Derecho. Dicho de otro modo, que los nombramientos del personal en procedimientos selectivos de la Oficina requerida, (en tanto que tienen una indudable trascendencia económico-financiera), se han llevado conforme a los procedimientos que los regulan y en caso de no ser así, informar de ello y en su caso, proponer actuaciones. A efectos comparativos, se citan dos informes del Tribunal de Cuentas en los que se requiere información sobre procedimientos de concurrencia competitiva, y que a priori podían no considerarse procedimientos de contenido económico, pero que, indudablemente tienen trascendencia económico-financiera y contable, pues suponen la realización del gasto que tiene asignado el organismo del sector público de que se trate. Es decir, el control ejercido es sobre la "legalidad" del gasto que se imputa a un presupuesto público.

Por lo tanto, el tratamiento que se deriva del requerimiento analizado encuentra su legitimación en el artículo 6.1 e) del RGPD y además se estima conforme a los principios de limitación de finalidad y minimización, en relación con las competencias que tiene atribuidas la Sindicatura y la finalidad a la que responde sus funciones. Como en el anterior informe, se recuerdan los requisitos que debe cumplir los requerimientos de

información que realizan las autoridades públicas en el ejercicio de sus funciones.

En otro orden de cosas, procede citar el **Informe 57/2022 en el que por parte de la Dirección General de Tráfico se solicita el criterio de la AEPD en relación con la licitud de proporcionar a las compañías que gestionan aparcamientos privados, la información que consta en el Registro de Vehículos sobre el domicilio de los titulares de los vehículos que hacen uso del aparcamiento, con objeto de poder reclamarles, en su caso, el importe no abonado, con base en su interés legítimo derivado del contrato de depósito del vehículo.**

El informe analiza el contenido y la naturaleza del Registro de Vehículos, indicando que tiene un carácter meramente administrativo y no civil, en el sentido de que no atribuye la propiedad del vehículo a su titular, como tampoco puede determinarse que quién consta como titular sea el conductor del vehículo en cuestión. Lo que es importante de cara a la adecuación al juicio de proporcionalidad que según reiterada doctrina del Tribunal Constitucional ha de superar cualquier medida restrictiva de derechos fundamentales, y que se concreta en tres ámbitos, la idoneidad, la necesidad y la proporcionalidad en sentido estricto.

El juicio de idoneidad ha de ser necesariamente negativo, ya que la medida propuesta no sirve al propósito perseguido, esto es, el acceso a determinados datos de carácter personal —tales como el domicilio— del titular de un vehículo no conduce, necesariamente, a la obtención de información personal del conductor cuya inobservancia contractual se persigue.

Respecto del juicio de necesidad, se indica que el fin perseguido puede alcanzarse de una manera menos intrusiva, teniendo en cuenta la protección de los datos de carácter personal, existiendo otros medio más moderados para la consecución de tal propósito con igual eficacia tales como el establecimiento de barreras, o la intervención del personal del aparcamiento, que, además de resultar más efectivos, no requieren del tratamiento del dato personal relativo al domicilio de una persona que no siempre coincide con el dato relativo al domicilio del usuario del aparcamiento.

Finalmente, respecto del juicio de proporcionalidad en sentido estricto, el acceso pretendido a la información obrante en los registros de la DGT no resulta proporcional, al no devenir equilibrado en atención a la ponderación entre la finalidad perseguida y el grado de restricción del derecho fundamental a la protección de datos de carácter personal. Esto es, de dicha medida podrían derivar más perjuicios sobre la protección de los datos de carácter personal de los titulares de los vehículos, cuyos domicilios resultarían accesibles a la consultante, que beneficios o ventajas para la compañía que explota el aparcamiento.

En consecuencia, en el supuesto no concurre ninguno de los tres requisitos mencionados en relación con las exigencias derivadas del principio de proporcionalidad.

En cuanto al interés legítimo que se plantea en la consulta, el informe recuerda lo indicado en el Informe 50/2019 sobre el acceso y cesión de datos personales del padrón municipal señalando que “la comunicación de datos al amparo de lo previsto en el artículo 6.1.f) del RGPD requiere la realización de la correspondiente prueba de sopesamiento con el fin de determinar si el interés legítimo del solicitante prevalece sobre el derecho a la protección de datos de los afectados, lo que supone que, por parte del responsable del tratamiento: a) debe valorarse el interés legítimo invocado por el solicitante, atendiendo a la concreta finalidad para la que se solicite el certificado o volante de empadronamiento. b) debe atenderse igualmente a la especial situación en la que puedan encontrarse los afectados. c) en cuanto al requisito de la ponderación de los derechos e intereses en conflicto, ésta dependerá, en principio, de las circunstancias concretas del caso particular de que se trate. Para la adecuada ponderación, es necesario que el responsable disponga de toda la información necesaria lo que supone, no sólo conocer la finalidad para la que se solicitan los datos, sino, muy especialmente, la incidencia que pueda tener en la esfera del afectado su comunicación, lo que implica el

cumplimiento del deber de información en el momento de la obtención de los datos previsto en el artículo 13 del RGPD y el posible ejercicio por el afectado de su derecho de oposición al amparo del artículo 21 del mismo."

Finalmente, concluye señalando que el análisis de la legitimidad del acceso a los datos personales que se pretende y la valoración de si dicho acceso supone o no un tratamiento excesivo, deben realizarse examinando tanto el principio de finalidad como el principio de proporcionalidad, sin que en el supuesto planteado se cumplan los requisitos inherentes a dichos principios. A su vez, lo dispuesto en la Disposición adicional décima de la LOPDGDD en relación con las comunicaciones de datos realizadas por los sujetos enumerados en su artículo 77.1, no resulta aplicable al supuesto planteado en la consulta dado que, de una parte, (i) no se cuenta con el consentimiento de los afectados, y, de otra parte (ii), no se aprecia que concurra en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del RGPD

Otro aspecto que tradicionalmente se ha tratado en las consultas recibidas es el referente al rol que deben desempeñar las entidades en relación con su intervención en un determinado tratamiento datos personales, es decir, ya sea como responsables del tratamiento, ya sea como encargado del tratamiento.

Así en el **Informe 58/2022** se plantea qué condición debe tener una entidad que presta servicios en el área de la construcción, referidos a control técnico, certificados de conformidad, prevención para empresas, coordinación en materia de seguridad y salud, asistencia en la gestión de riesgos operacionales, y control de calidad.

Actualmente es el promotor de las obras y servicios arrendados el que es considerado responsable del tratamiento, y la consultante, encargada del tratamiento respecto al acceso y comunicaciones del flujo de datos personales que se generan en las obras, si bien se plantean dudas en este sentido por su posible encaje dentro de la figura de responsable del tratamiento aludiendo a que parte de las funciones encomendadas se realizan en virtud de obligaciones legales a lo que hay que añadir que las comunicaciones de datos personales resultan necesarias para el cumplimiento de la relación contractual suscrita con el promotor.

La cuestión que debe dilucidarse es la determinación del papel de cada uno de los intervinientes en el proyecto y ejecución de la obra desde el punto de vista de la normativa de protección de datos de carácter personal, a fin de especificar si dichos intervinientes tienen la condición de responsables o de encargados del tratamiento, siendo importante señalar que la condición de responsable no exige el acceso efectivo a los datos, sino la potestad de decisión sobre los fines y los medios del tratamiento —ex art 4.7 RGPD—. Para lo que se analizan los artículos 2, 3 y 4 del del Real Decreto 1627/1997, de 24 de octubre, por el que se establecen disposiciones mínimas de seguridad y de salud en las obras de construcción y se ponen en conexión con las Directrices 7/2020 sobre Responsable y Encargado, adoptadas de forma definitiva el 7/07/2021 del Comité Europeo

de Protección de Datos concluyendo que siendo el responsable del tratamiento quien determina los fines y los medios de este, es preciso analizar cómo se articulan dichas decisiones.
Para ello, debe partirse de la definición del promotor como (i) "persona física o jurídica por cuenta de la cual se realice una obra" (artículo 2.1.c. Real Decreto 1627/1997), (ii) siendo dicho promotor quien designa un coordinador en materia de seguridad y de salud durante la elaboración del proyecto de obra (artículo 3.1), y (iii) procede —asimismo— a su designación durante la ejecución de la misma (artículo 3.2), (iv) sin que la designación de los coordinadores exima al promotor de sus responsabilidades (artículo 3.4). Asimismo, las obligaciones atinentes a la elaboración del estudio de seguridad y salud o del estudio básico de seguridad y salud en las obras corresponden también al promotor (artículo 2 Real Decreto 1627/1997), sin perjuicio de que este proceda a la designación de otra persona o entidad, a la que encargue la gestión de dichos trabajos, su puesta en marcha y su seguimiento.
En este escenario, tiene encaje la figura del coordinador en materia de seguridad y de salud —CSSFE— designado por el promotor (artículo 2.1 e. y f.), que, tanto durante la elaboración del proyecto de obra como durante su ejecución (artículo 3), actuará por delegación, en calidad de encargado del tratamiento.

En consecuencia, las funciones y tareas encomendadas a los CSSFE que sean contratados por el promotor al amparo de los artículos 2 y 3 del Real Decreto 1627/1997, de 24 de octubre, se llevarán a cabo siempre por cuenta de dicho promotor, quien, en su ámbito organizativo y, de acuerdo con los fines previstos para el tratamiento de los datos personales, optará por la contratación de una u otra persona física o jurídica para la realización de los correspondientes trabajos, siendo estos de cuenta y riesgo del promotor de la obra, que no queda exonerado de sus obligaciones.

De tal suerte, nos encontramos ante un claro ejemplo de encargado del tratamiento, accediendo los CSSFE a los datos por cuenta del responsable de este. Incluso en este supuesto en el que realiza sus funciones con total imparcialidad e independencia, siguiendo lo dispuesto en la normativa que, específicamente, resulta aplicable—, (i) procesa los datos personales en beneficio del responsable, (ii) y realiza el tratamiento en nombre de dicho responsable, aunque no se encuentre bajo su autoridad o control directo, pero (iii) sirviendo a los intereses del promotor (responsable).

Finalmente se indica que la base jurídica que legitima el tratamiento que realice, tanto responsable como encargado es la prevista en el artículo 6.1 c) RGPD, por cuanto es una obligación legal del promotor, dimanante de lo previsto en los artículos 2, 3 y 4 del Real Decreto 1627/1997, de 24 de octubre, por el que se establecen disposiciones mínimas de seguridad y de salud en las obras de construcción, dictado en desarrollo del artículo 6 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

Por último indicar que en el siguiente epígrafe dedicado a la actividad del Gabinete Jurídico de la AEPD se aborda el listado de los informes preceptivos sobre disposiciones de carácter general emitidos durante el ejercicio, resaltando que, como se indicó en lo hitos de esta memoria, en ellos se sigue insistiendo en la necesidad de que se realice por parte del del órgano proponente de la norma de que se trate, el correspondiente análisis de riesgos y en su caso, evaluación de impacto y se incorpore en la propia norma o bien a través de disposiciones adicionales o bien se incorpore en la memoria de análisis de impacto normativo (MAIN) que se acompañe al proyecto normativo en cuestión.

Sirva citar por todos, el **Informe 86/2022** que señala que para el adecuado establecimiento de dichos límites -a la injerencia en el derecho fundamental- y la correcta identificación de las garantías que deban trasladarse al texto legal, la Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en

el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, realice un análisis de riesgos y, en su caso, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo (MAIN). Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto "Otros impactos", el análisis del "impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma": La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.. Su realización permitiría que los responsables o encargados del tratamiento, una vez promulgada la norma, no tendrían la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general. La Agencia recuerda, asimismo, que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta "los riesgos que se derivan del tratamiento de los datos personales" (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

2.2.2. 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. Entre las disposiciones informadas en el año 2022 cabe mencionar las siguientes:

- Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 2-2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo.
- Anteproyecto de Ley Orgánica del Derecho de Defensa.
- Anteproyecto de ley de creación autoridad administrativa independiente para la investigación técnica de accidentes.
- Anteproyecto de ley por el que se modifica el texto refundido de la Ley General de derechos de las personas con discapacidad y su inclusión social, aprobado por RD legislativo 1/2013 de 29 de noviembre, con el objeto de extender la condición legal de persona con discapacidad a determinados pensionistas.
- Anteproyecto de ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, por la que se transpone la Directiva (UE) 2019/1937.
- Anteproyecto de ley de Protección, Derechos y Bienestar de los Animales.

- Anteproyecto de Ley en materia de requisitos de Accesibilidad de determinados productos y servicios.
- Anteproyecto de Ley de Empleo.
- Anteproyecto de Ley de lucha contra el dopaje animal en las competiciones deportivas.
- Anteproyecto de Ley de información clasificada.
- Anteproyecto de Ley por la que se crea la Agencia Estatal de Salud Pública.
- Anteproyecto de Ley de creación de la autoridad administrativa independiente de defensa del cliente financiero.
- Anteproyecto de Ley de Transparencia e integridad en las actividades de los grupos de interés.
- Anteproyecto de Ley de Familias.
- Proyecto de Real Decreto por el que se establece y regula el Sistema de información de explotaciones agrícolas y ganaderas y de la producción agraria.
- Encuesta Estructural a Hogares.
- Proyecto de Real Decreto por el que se desarrollan entornos más seguros de juego.
- Proyecto de Real Decreto por el que se establece el procedimiento para el reconocimiento, declaración y calificación del grado de discapacidad.
- Proyecto de Real Decreto normas reguladoras Bono Cultural Joven.
- Proyecto de Real Decreto por el que se crea el Registro de Titularidades Reales y se Aprueba su Reglamento.
- Proyecto de Real Decreto por el que se establece el marco general del banco de pruebas regulatorio para el fomento de la investigación y la innovación en el sector eléctrico.
- Proyecto de Real Decreto por el que se modifica el RD 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trecientos sesenta y cinco días de su duración.
- Proyecto de Real Decreto por el que se regulan las condiciones básicas de accesibilidad y no discriminación de las personas con discapacidad para el acceso y utilización de los bienes y servicios a disposición del público.
- Proyecto de Real Decreto por el que se establecen los criterios de calidad y seguridad de las unidades asistenciales de radioterapia.
- Proyecto de Real Decreto por el que se desarrolla el Reglamento de Adopción Internacional.
- Proyecto de Real Decreto por el que se regulan las comunicaciones de emergencia a través del número único de emergencia 112.
- Proyecto de Real Decreto por el que se regula el Registro de Contratos Alimentarios.
- Proyecto de Real Decreto por el que se regula el sistema de transmisión de alertas públicas mediante servicios móviles de comunicaciones electrónicas en caso de grandes catástrofes o emergencias inminentes o en curso.
- Proyecto de Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 11/2021, de 28 de diciembre de Lucha contra el Dopaje en el Deporte.
- Proyecto de Real Decreto por el que se regula la organización y funcionamiento de los registros nacionales den materia de reproducción humana asistida.

- Modificación del RD 453/2020, de 10 de marzo, por el que se desarrolla la estructura básica del Ministerio de Justicia y se modifica el Reglamento del Servicio Jurídico del Estado, aprobado por RD997/2003, de 25 de julio.

- Proyecto de RD por el que se aprueba el reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales y la estandarización de formatos de los registros de facturación.

- Proyecto de Real Decreto datos Informes clínicos del Sistema Nacional de Salud.

- Proyecto de Real Decreto por el que se modifica el Real Decreto 1850/2009 de 4 de diciembre, sobre expedición de títulos académicos y profesionales correspondientes a las enseñanzas establecidas por la Ley 2/2006 de 3 de mayo, de Educación.

- 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 sordociegos.

- Proyecto de Real Decreto por el que se modifican el Reglamento general de desarrollo de la Ley 58/2003, el Reglamento general de Recaudación, etc.

- Proyecto de Real Decreto sobre la inscripción de las personas de nacionalidad española en los Registros de matrícula de las Oficinas Consulares en el extranjero.

- Proyecto de Orden Ministerial por la que se regula el funcionamiento del registro electrónico de la Secretaría de Estado de la Seguridad Social y Pensiones.

- Subsanación y anexos al proyecto de Orden Ministerial Movimientos efectivo.

- Proyecto de Orden Ministerial por la que se crea una Oficina de Asistencia en materia de Registros del Ministerio de Sanidad.

- Proyecto de Orden Ministerial por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Consumo.

- Proyecto de Orden Ministerial por la que se establecen las condiciones de la integración del Nodo SNSFarma en el repositorio nacional.

- Proyecto de Orden Ministerial por la que se regula la información a remitir por los prestadores de servicio de recarga energética al Ministerio para la Transición Ecológica y el Reto Demográfico, a las Comunidades Autónomas y la Ciudades de Ceuta y Melilla.

- Proyecto de Orden Ministerial por la que se modifica la Orden ESS/1187/2015, de 15 de junio, que desarrolla el RD 625/2014, de 18 de julio, que regula determinados aspectos de gestión y control de procesos por incapacidad temporal en los primeros 365 días.

- Proyecto de Orden Ministerial por la que se establece el sistema HEBAR como herramienta epidemiológica ambiental basada en el control de las aguas residuales.

- Proyecto de Orden Ministerial por la que se establece un sistema de identificación del personal con funciones de inspección de Sanidad Exterior.

- Proyecto de Orden Ministerial por la que se aprueba la Política de Seguridad de la Información del Ministerio de Asuntos Económicos y Transformación Digital.

- Proyecto de Orden Ministerial por el que se establece y abre el procedimiento para el reconocimiento y la expedición de la acreditación de proyectos de interés singular para la formación profesional elaboradas y presentadas por empresas, organismos y entidades.

- Proyecto de Orden Ministerial por la que se aprueba la política de seguridad de la información y de los servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las tecnologías de la información y las comunicaciones del departamento.

- Proyecto de Circular del Banco de España, por la que se modifica la Circular 1/2013 de 24 de mayo, del Banco de España sobre la Central de Información de Riesgos.

2.2.3. 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.

En este apartado se recogen, por un lado, las Sentencias de la Audiencia Nacional, que es órgano judicial competente para conocer de los recursos interpuestos contra las resoluciones de la AEPD, y en su caso, las Sentencias del Tribunal Supremo que conocen de los recursos de casación que se interpongan contra las Sentencias de la Audiencia Nacional. Y por otro, se incluye aquella jurisprudencia del Tribunal Constitucional y de los Tribunales Europeos que versen sobre la materia y que por su interés merecen ser destacadas.

Durante el año 2022 se han dictado por la Sala de lo contencioso-administrativo de la Audiencia Nacional, 59 resoluciones[1], de las cuales: 40 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas) (68 %); 3 estimaron parcialmente los recursos (5%); 6 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia (10%); y 10 inadmitieron los recursos interpuestos contra resoluciones de la Agencia (17%).

Por su parte, el Tribunal Supremo dictó una resolución que confirma el criterio de la AEPD. Asimismo, hay que destacar que el Tribunal Constitucional resolvió un recurso de amparo que estima las pretensiones del afectado y que confirman el criterio que la AEPD había sostenido en el caso concreto.

En cuanto a los sectores de actividad de los recurrentes tanto en la Audiencia Nacional como en el Tribunal Supremo, de 69 resoluciones[2] que resuelven recursos frente a las resoluciones de la AEPD, y en su caso, frente a Sentencias de la Audiencia Nacional que confirman las resoluciones de la AEPD, la mayor parte han sido interpuestos por particulares (50)

No obstante, un alto número de ellas son desestimatorias, siendo el motivo más común la falta de indicios o inconsistencia fáctica y jurídica de la denuncia, que desaconsejan si quiera iniciar actuaciones de investigación, tal como también aprecia tribunal. También se observa un aumento significativo en las que el fallo es la declaración de inadmisibilidad del recurso por falta de legitimación activa por cuanto se solicita al tribunal a quo, no sólo la revocación de la resolución de la AEPD sino la imposición de una sanción, recordándose por la Sala la ausencia en los particulares de un derecho subjetivo en ese sentido, reiterando la doctrina de que el ius puniendi no está en manos de los particulares.

Asimismo, entre las desestimatorias, procede citar aquellas que versan sobre el ejercicio de derechos, que confirman el criterio de la AEPD por cuanto se considera que el responsable ha dado respuesta válida en derecho al titular de los datos personales, siendo una cuestión distinta

[1] Únicamente se refiere a Sentencias, quedando por tanto excluidos otro tipo de resoluciones de los Tribunales como Autos, Decretos, Diligencias de Ordenación, etc., que resuelven aquellos procedimientos en los que se ha producido el desistimiento, la caducidad o el archivo por falta de postulación, o tratan de medidas cautelares,

[2] Aquí se incluyen todo tipo de resoluciones (sentencias, autos, providencias, etc. tanto de la Audiencia Nacional como del Tribunal Supremo)

que dicha respuesta no satisfaga los intereses particulares del afectado, y aquellas en las que se pone el acento en los requisitos formales de la solicitud del derecho o en el carácter repetitivo de la misma.

Destacan las del sector de las Telecomunicaciones (5) de banca y seguros (3), el sector de los sistemas de información crediticia (3) y con el mismo número de resoluciones el sector de distribución y venta, y el de agua y energía. Los restantes sectores como administraciones públicas, asociaciones sindicales, sociedad de la información o publicidad y prospección comercial son los menos significativos cuantitativamente y han sufrido una disminución respecto del ejercicio anterior.

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

Comenzando por la aplicación de los principios en el tratamiento de datos, y en concreto el de licitud, hay que citar un primer grupo de resoluciones que abordan el tratamiento realizado por las autoridades al amparo de los apartados e) y c) del artículo 6.1 del RGPD, y en concreto por la Agencia Estatal de la Administración Tributaria (AEAT)

La Sentencia de la Audiencia Nacional de 28 de abril de 2022 que resuelve el Recurso nº. 224/2021, interpuesto por un particular contra la Resolución de inadmisión.

Se denuncia por la recurrente que la AEAT, en el marco de un procedimiento de inspección tributaria contra un tercero, ha emitido acuerdos de liquidación de IVA y de IRPF donde constan sus datos personales no siendo interesada en dichas actuaciones, y por tanto se ha producido una cesión de datos personales de la recurrente en favor de la obligada tributaria por parte de la AEAT. En concreto, indica que en los citados acuerdos de liquidación se menciona a la reclamante con su nombre y apellidos, DNI, se hace referencia a sus vínculos familiares con terceras personas, se desvelan datos de carácter patrimonial y económicos al mencionar a la reclamante como titular de un estanco y administradora de una sociedad de responsabilidad limitada, datos que no eran conocidos en su totalidad, con anterioridad a la notificación de los acuerdos de liquidación, por la obligada tributaria.

La postura del Abogado del Estado se concretaba en que los acuerdos de liquidación responden a la competencia que tiene atribuida la Administración tributaria en orden a la aplicación de los tributos, así como al cumplimiento de la obligación que pesa sobre la misma en cuanto a la motivación de las liquidaciones tributarias, ex artículo 102.2.c) Ley General Tributaria.

En estos términos, indica que en los acuerdos de liquidación se cuestiona por la AEAT las facturas de gastos procedentes de la entidad donde es administradora la recurrente, como proveedor de servicios de la obligada tributaria y al objeto de fundamentar la obligación legal de la Administración de justificar la no deducción por parte de la misma de los gastos que le habían sido facturados por la entidad donde es administradora la recurrente, resultaba imprescindible poner de manifiesto la actividad y operaciones del resto de estancos de personas vinculadas familiarmente, al objeto de fundamentar la instrumentalización de dicha entidad para disminuir la tributación de las personas titulares de los estancos y de la propia sociedad registrando gastos que en realidad son personales de los administradores y familiares (entre ellos la recurrente).

Pues bien, la Sala tras indicar que son de aplicación los artículos 6.1 c) y e) del RGPD y 8 de la LOPDGDD, recuerda lo indicado en el artículo 95.1 de la LGT que alude al carácter reservado de los datos tributarios en poder de la Administración tributaria, destacando que solo pueden ser utilizados con fines tributarios dentro de sus funciones y en el marco o ámbito de sus competencias.

En consecuencia, los acuerdos de liquidación, referidos a la obligada tributaria, responden a la competencia que tiene atribuida la Administración tributaria en orden a la aplicación de los tributos y que se desarrolla, “a través de los procedimientos administrativos de gestión, inspección y recaudación y los demás previstos en este título.”, artículo 83.3 LGT.

Liquidaciones tributarias que la Administración tributaria tiene obligación de motivar "cuando no se ajusten a los datos consignados por el obligado tributario o a la aplicación o interpretación de la normativa realizada por el mismo, con expresión de los hechos y elementos esenciales que las originen, así como de los fundamentos de derecho." (art. 102.2.c) LGT).

En efecto, para motivar de forma suficiente y acreditar por parte de la Administración tributaria las razones del rechazo de los citados gastos resultaba imprescindible consignar los datos personales que se plasmaron en dichos acuerdos, entre otros, NIF, nombre y apellidos, administradora de la sociedad etc., Ello permitía poner de relieve esas vinculaciones familiares y con la sociedad, que se consideraban determinantes, junto con otros datos, de la falta de justificación de lo facturado por la sociedad de la que era administradora la recurrente a la obligada tributaria.

Por tanto, no se trata de que los datos de la recurrente incluidos en los acuerdos de liquidación en cuestión se hayan cedido a un tercero (obligado tributario), sino que dichos datos se han utilizado por parte de la AEAT en el ejercicio de sus funciones y de las potestades atribuidas a la Administración tributaria al servicio de los intereses públicos, con fines tributarios, con el objeto de fundamentar, como resulta legalmente exigible, la instrumentalización de la sociedad de la que era administradora la recurrente para disminuir la tributación, entre otras personas, de la obligada tributaria y justificar, en suma, porque no consideraba deducibles el importe de las facturas de gastos de la citada sociedad que la misma pretendía.

Por lo tanto, el fallo de la sentencia es desestimatorio confirmándose la resolución de la AEPD. En idénticos términos se dicta la **Sentencia de la misma fecha recaída en el Recurso nº 227/2021** y que se refiere a otro de los administradores de la sociedad instrumental para la atribución de los gastos irregulares de los impuestos IVA e IRPF que se han analizado en la anterior resolución.

Siguiendo con los principios del tratamiento, las siguientes resoluciones abordan situaciones en las que se ve afectado el principio de licitud por cuanto se denuncia el uso de datos personales para la contratación se productos o servicios o para la modificación de contratos ya existentes, es decir, para contratación fraudulenta.

La **Sentencia de la Audiencia Nacional de 18 de noviembre de 2022 recaída en el Recurso nº 590/2022** interpuesto por una entidad comercializadora de energía contra una resolución sancionadora.

Los hechos de los que trae causan la sanción impuesta son el tratamiento de los datos personales de un afectado por parte de la entidad para darle de alta en un contrato de energía en una vivienda respecto de la que no tiene ninguna vinculación.

El afectado tras recibir una factura con sus datos personales y un teléfono fijo que no le corresponde,

sobre un punto de suministro de una vivienda que no reconoce, realizó una llamada con su teléfono móvil a la entidad para reclamar lo sucedido. Días más tarde recibe un contrato para devolver firmado dónde consta el número de teléfono móvil con el que hizo la primera reclamación.
La entidad manifiesta que los datos del afectado fueron facilitados por una tercera persona que realizo una llamada y afirmó actuar en representación del afectado.

La resolución de la AEPD analiza los artículos 5 y 6 del RGPD y concluye que la entidad trató los datos personales del reclamante sin legitimación, y sin que conste que haya tratado los datos personales del reclamante de manera lícita. Destaca la resolución que de las grabaciones se prueba el origen de algunos de los datos personales del reclamante facilitados por una tercera persona a la entidad, pero no de otros. Así la entidad trató datos vinculados a un contrato del que es ajeno el titular, y su domicilio en su localidad no coincide con el punto de suministro y el nº móvil del reclamante que la entidad incorpora al ejemplar del contrato lo facilitó el reclamante al llamar a la misma para comprender la situación, siendo dicha entidad quien lo incorpora al contrato. No fue la tercera persona quien facilitó el domicilio del reclamante dónde la citada entidad envió el contrato. No se aporta documento alguno que acredite la representación de la tercera persona, ni nunca lo exigió, no ha desplegado la más mínima diligencia para la comprobación de los datos y de la representación que se atribuye la persona que llama por teléfono.

La Sala resuelve desestimando el recurso contra la resolución sancionadora, por considerar que ha habido un tratamiento de datos personales sin que se diera ningún supuesto de legitimación de acuerdo con el artículo 6.1 del RGPD. No puede entenderse celebrado el contrato que permitiría la aplicación del apartado b) de dicho artículo, pues no se acredito que la persona que pretendió el cambio del contrato y proporcionó los datos del afectado, actuara en representación de este, ya que, si bien el mandato verbal no exige una forma concreta (artículos 1709 y ss. del Código Civil), no puede presumirse y hay que acreditar su existencia. Asimismo analizando el elemento subjetivo en la comisión de la infracción al indicar que existe una responsabilidad en una entidad comercializadora y suministradora de servicios como es la actora que está encargada de un fichero y que no actúa de una manera diligente cuando sin exigir ninguna acreditación acepta una representación inexistente, pretendiendo eludir esa responsabilidad basada en la existencia de una representación que no acredita cuando conforme a las reglas generales de la carga de la prueba le hubiera correspondido demostrarla. En consecuencia, la entidad sancionada actuó cuando menos con negligencia y de ahí deriva su responsabilidad. Y por último, también se aborda la adecuación de la sanción en relación con el principio de proporcionalidad al indicar que la sancionada se ha mostrado reticente a llevar a cabo una regularización de las circunstancias sobre la base de la existencia de una representación sin acreditar cuando a ella le era exigible esa prueba en virtud de la carga de la prueba de los hechos positivos. Además, de no contar con esa representación, la entidad emitió notificaciones de impago por lo que parece una actuación automática de la entidad sin velar por el cumplimiento estricto de la protección de datos que le incumbía.

En términos similares a la anterior, la **Sentencia de la Audiencia Nacional de 17 de febrero que resuelve el Recurso nº 650/2020** interpuesto frente a la resolución sancionadora, en la que se aborda un supuesto de representación de un tercero, que la entidad sancionada no verifica dicha representación y en consecuencia se confirma el criterio de la AEPD.

También referida al fraude en la contratación procede destacar la **Sentencia de la Audiencia Nacional de 1 de julio de 2022 que resuelve el Recurso nº 405/2021** interpuesto frente a la resolución sancionadora, que focaliza el debate en la relación responsable y encargado del tratamiento y las medidas adoptadas para verificar la contratación que forma parte de los servicios encomendados.

Se aduce por la parte recurrente que existía un contrato de prestación de servicios de telemarketing con la entidad A, y que dicha entidad en

el marco de los servicios acordados efectuaba llamadas comerciales sirviéndose de su propia base de datos de contactos, identificándose como responsable del tratamiento ante los mismos, ofreciendo los servicios de la recurrente. En virtud de dicho contrato, la entidad A trataba los datos de sus contactos en su propio nombre y por su cuenta a través de sus propias redes comerciales mediante llamadas telefónicas (telemarketing), actuando en calidad de responsable del tratamiento y, cuando un usuario se mostraba interesado en la contratación de los servicios de la recurrente, transfería la llamada a un teleoperador. Una vez obtenida la confirmación del cliente, grabado el consentimiento y habiendo dado cumplimiento a todos los requisitos exigidos por la normativa en relación con los procesos de contratación a distancia, la Entidad A se comprometía a volcar en los sistemas de información de la recurrente, los datos del nuevo cliente junto con la grabación a fin de que se llevase a cabo el alta del servicio. Se resalta, que el 8 de enero de 2020, dicha entidad volcó en los sistemas de la recurrente los datos de la denunciante como nuevo cliente, y a raíz de la reclamación efectuada por la nieta de la denunciante, se dio de baja el contrato el 21 de enero de 2020, una vez que la reclamante gestionó su alta en otra comercializadora, siéndole notificada dicha baja a la interesada mediante carta el 22 de enero de 2020.

Entiende que ha existido una actuación fraudulenta de la entidad A ya que no siguió sus instrucciones, lo que lleva a considerar a dicha entidad como responsable del tratamiento de acuerdo con el artículo 28.10 del RGPD. Se alude que hasta que tuvo conocimiento del fraude cometido por la Entidad A, actuó con toda la diligencia posible y al amparo de la existencia de una relación contractual de acuerdo con el articulo 6.1 b) del RGPD.

La Sala analiza el contrato entre ambas entidades e indica que se hace constar que la Entidad A, recabaría datos del cliente, como su nombre, D.N.I., número de teléfono, correo electrónico, IBAN para domiciliación de recibos, dirección completa de suministro y facturación… Y dicha entidad informaría en las aplicaciones de la parte actora dichos datos, así como la documentación necesaria para la contratación, enviando al cliente su contrato, a través de la aplicación de la parte actora, encargándose la Entidad A de la verificación y autentificación del consentimiento contractual de los nuevos clientes, debiendo subir a la aplicación de la parte recurrente la grabación íntegra y sin cortes del proceso de venta, señalándose que sin esta grabación subida a los sistemas de la recurrente no tendría validez alguna el contrato de venta telefónica.

Resalta que la recurrente no adoptó ninguna clase de medida o de cautela con la empresa subcontratada a la que encomendó la realización de contrataciones ya que debió verificar la grabación que subió a su aplicación la entidad A, así como la documentación, teniendo en cuenta que podía examinar en cualquier momento, el cumplimiento de las obligaciones de la citada entidad derivadas del contrato, y la adecuación de la prestación de los servicios en los términos pactados y a las instrucciones impartidas por la parte recurrente.

Concluye la Sala que ninguna de las circunstancias concurrentes en el caso que nos ocupa, permite excluir este elemento subjetivo de la infracción, debiéndose señalar que no consta que la recurrente, hubiese adoptado las medidas adecuadas y eficaces que le permitiesen identificar inequívocamente al cliente que realizó el cambio de comercializadora de electricidad.

Siguiendo con el principio de licitud en el ámbito de las acciones de mercadotecnia procede citar la **Sentencia de la Audiencia Nacional de 9 de diciembre de 2022 que resuelve el Recurso nº 1994/2021** interpuesto contra la resolución sancionadora de la AEPD, por el tratamiento ilícito de los datos del afectado en relación con los artículos 6.1 f) y 21 del RGPD.

La Sentencia aborda también otras cuestiones al margen del fondo del asunto que resulta procedente destacar. Por un lado, se analiza la legalidad de la adopción de la resolución por la Directora de la AEPD una vez expirado su mandato sin que se haya procedido a la renovación, lo que a juicio del recurrente conlleva a la nulidad de pleno derecho por la adopción de una resolución sin compe-

tencia para ello (artículo 47.1 de la Ley 39/2015, de 1 de octubre). Y por otro, la adecuación a los principios del derecho sancionador, referidos a la determinación "in audita parte" en el acuerdo de inicio del procedimiento sancionador de la cuantía de la sanción a imponer, pudiendo vulnerarse el derecho de defensa, y contaminando por el órgano competente para resolver, la actuación inspectora y la actividad del órgano instructor, pues ya el acuerdo de inicio muestra el resultado que debería tener el procedimiento.

Respecto de la primera cuestión, la Sala indica que de acuerdo con el artículo 36.1 de la Ley Orgánica 15/1999, de 13 de diciembre (LOPD), que es la normativa vigente cuando se efectúa el nombramiento de la Directora de la AEPD, transcurrido el término de 4 años, el Gobierno puede cesar al Director sin necesidad de causa, pero ello no implica que cuando se cumple ese plazo su cargo automáticamente deje de tener efectividad y de tener funciones o competencia alguna, pues eso no resulta expresamente de la citada LOPD, ni tampoco de la Ley Orgánica 3/2018. de 5 de diciembre (LOPDCDD), en su art. 48 respecto de la Presidencia de la AEPD. Así se ha entendido y venido haciendo por todos los Gobiernos que proceden a cesar expresamente a los Directores de la AEPD mediante Real Decreto, aún, cuando su plazo de nombramiento hubiera expirado, sin que sus cargos dejasen de tener efectividad, en funciones, hasta sus respectivos ceses y los coetáneos nombramientos de sus sucesores en el cargo, para evitar vacíos en la institución. El legislador podía haber establecido expresamente la previsión automática de decaimiento del cargo, esto es, que la efectividad en el cargo cesa en el mismo momento del cumplimiento del plazo, pero no lo ha hecho ni en la LOPD ni en la vigente LOPDGDD, ni tampoco en el RD 389/2021, de 1 de junio de 2021, por el que se aprueba el nuevo Estatuto de la AEPD. Por tanto, no habiéndose establecido limitaciones a la actuación del Director de la AEPD en funciones la Directora de la AEPD ostenta competencia para dictar la resolución impugnada, así como el acuerdo de inicio del procedimiento sancionador.

En cuanto a la segunda cuestión, la Sala indica que el artículo 64.2 de la Ley 39/2015, de 1 de octubre, exige la constancia en el acuerdo de incoación de, al menos, los hechos, su posible calificación y de las posibles sanciones a imponer, así como de informar, ya de inicio, de la posibilidad de aplicar las reducciones que permite el artículo 85 de la LPACAP, que presupone una determinación provisional inicial de las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción. Así las cosas, a la vista de los citados preceptos y siguiendo el criterio de la SAN, Sec. 3ª, de 19 de junio de 2019 (Rec. 447/2018) en un supuesto similar al presente: "No existe por tanto impedimento legal alguno para que el acuerdo de incoación contenga una concreción inicial y provisional de la sanción/es que pueda/n aparejar los hechos investigados dentro de las previstas normativamente, lo que no implica merma derechos del expedientado pues ello se hace "sin perjuicio de lo que resulte de la instrucción (…) y, esta concreción inicial y provisional, en aras a la celeridad y eficacia en el obrar administrativo, viene a permitir el pago voluntario desde el mismo momento del inicio (…). No hay base legal alguna para entender que la concreción de la sanción y el juego del pago voluntario no puedan producirse hasta la propuesta de resolución tras la correspondiente instrucción". Es decir, la competencia para determinar el acuerdo de inicio del procedimiento sancionador determina la obligación de que dicho acuerdo ha de contener la totalidad de las circunstancias previstas por la normativa aplicable, entre ellas la determinación provisional de la sanción que pueda corresponder, que será sin perjuicio de lo que resulte de la instrucción del procedimiento. Instrucción del procedimiento cuya competencia corresponde al instructor y al secretario, que fueron designados en el dispositivo 2 del citado acuerdo, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo previsto en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

Concluye la Sala indicando que corresponde por tanto al interesado, a la vista del acuerdo sancionador, solicitar las pruebas que crea oportunas, realizar alegaciones, etc., sin que pueda apreciar-

se la existencia de indefensión y apreciar la vulneración alegada; además, la recurrente en ningún momento ha mostrado su voluntad de reconocer la responsabilidad por la infracción sancionada y acogerse a los efectos previstos en el artículo 85 de la LPACAP.

En cuanto al fondo del asunto, se aduce por la recurrente que no estamos ante ninguna infracción del principio de licitud por cuanto el tratamiento de datos personales se produce al amparo del artículo 6.1 b) del RGPD ya que el único tratamiento de datos del reclamante llevado a cabo en el presente caso consiste en la remisión de una comunicación postal en la que se contenía información acerca de los productos y servicios por él contratados. Indicando que el hecho de que la caratula del sobre en que se incluye dicha comunicación incorpore información acerca de la entidad reclamante e incluso de los productos y servicios que comercializa, no puede ser considerado tratamiento de datos personales en los términos definidos en el art 4.2 del RGPD, sino únicamente una decisión empresarial ajena al tratamiento de datos de la entidad.

La Sala rechaza este argumento indicando que no solo se está utilizando los datos para informarle sobre los productos contratados, sino que además se pretendía hacer llegar publicidad sobre hipotecas al constar en la comunicación que: "Cuesta mucho encontrar la casa de tus sueños. Por eso, te quitamos las comisiones de tu nueva hipoteca. Solo por tener tu nómina domiciliada y nada más. Te quitamos las comisiones de: "apertura", "amortización anticipada", "cancelación anticipada", "gastos de correo". Para que soñar cueste menos. Consulta condiciones en oficinas Bankia o Bankia.es".

Comunicación comercial publicitando una hipoteca de la entidad que tiene la consideración de marketing directo de la actividad financiera, por cuanto es una comunicación personalizada, esto es, dirigida a una persona perfectamente individualizada e identificada con su nombre y apellidos; que se envió al reclamante como cliente de la entidad que recibe su correspondencia físicamente en formato papel, así como al resto de clientes que reciben su correspondencia en el mismo formato - como la entidad recurrente ha venido afirmando desde el inicio-. Es decir, por la entidad se seleccionó, entre el público objetivo potencialmente destinatario de la publicidad, el integrado por clientes de la entidad financiera que reciben correspondencia en formato papel, lo que se encuadra en una actividad de marketing directo de la entidad financiera.

Teniendo en cuenta lo anterior, y lo dispuesto en el artículo 21 del RGPD sobre el derecho de oposición a las acciones de mercadotecnia, consta en los autos que el afectado se opuso al tratamiento de sus datos para estas finalidades en el año 2018, siendo confirmado por la entidad, y con posterioridad en el año 2020 es cuando se produce el tratamiento de sus datos con fines comerciales.

Sobre el principio de transparencia procede citar la **Sentencia de la Audiencia Nacional que resuelve el Recurso nº 1410/2019**, y que, si bien es de fecha 11 de octubre de 2021, fue notificada a la AEPD durante el ejercicio 2022, razón por la que se incluye en la presente memoria.

La Sentencia resuelve el recurso interpuesto por la Liga Nacional de Fútbol Profesional (LaLiga) contra la resolución sancionadora de la AEPD que impone una sanción de 250.000 euros por la infracción del principio de transparencia previsto en el artículo 5.1 a) del RGPD, derivado del uso de una aplicación para dispositivos móviles.

Los hechos son, en síntesis, que la entidad sancionada pretendía luchar contra el fraude en los derechos audiovisuales de emisiones de los partidos de fútbol, a través de una aplicación para dispositivos móviles para lo cual necesitaba utilizar el micrófono del dispositivo y la información sobre la geolocalización de éste.

El funcionamiento de la aplicación consistía en que durante la emisión de los partidos de fútbol organizados por La Liga, se producía en los dispositivos móviles de los usuarios la activación del micrófono y se captaba el sonido ambiente para compararlo con dicha emisión y si coincidían ambas se activaba la geolocalización a los efectos

de comprobar si la emisión captada por el dispositivo se estaba produciendo en un establecimiento o domicilio en los que se había contratado el servicio correspondiente, de tal forma que si la geolocalización no coincidía con el "mapa" de las contrataciones legales, se identificaba que en un determinada dirección, se estaba produciendo una visualización ilegal o "pirata" y por tanto se estaban vulnerando los derechos de emisión cuya explotación monetizaba LaLiga.

El funcionamiento del sistema incidía en múltiples elementos del derecho a la protección de datos. En primer lugar, sobre la mera existencia de tratamiento de datos personales. A este respecto por la entidad recurrente se negaba que estuviera produciendo, por cuando el sonido captado se sometió a un proceso que convertía el mismo en una huella digital inteligible y que solo se enviaba para la correspondiente comparación, sin que se almacenara ni en el dispositivo móvil ni en ningún otro lugar. Por lo tanto, no había tratamiento de datos personales, a lo sumo existiría un tratamiento de dato seudonimizado. En segundo lugar, aducía que en caso de que las informaciones recabadas pudieran ser consideradas datos personales, podría ampararse suficientemente en el cumplimiento de una misión de interés público o, cuando menos, en la consecución de un interés legítimo de la propia entidad y de los clubes de fútbol que la integran, dado que ha sido el propio legislador el que le ha atribuido la gestión de los derechos audiovisuales de los que son titulares sus integrantes como establece el Real Decreto-ley 5/2015; en el ejercicio de esta competencia, La Liga consideró que existía una importante fisura en dicha gestión y explotación como consecuencia, esencialmente, de la piratería y de la utilización ilegal de las formas de explotación, que suponen un fraude al sistema de comercialización que calcula en 400 millones de euros anuales que, prácticamente, suponen un tercio del producto de la comercialización de los derechos audiovisuales. En tercer lugar, en cuanto al principio transparencia, el recurrente alegaba que no se exigía ni en el RGPD ni en las Directrices del Grupo de Trabajo del Articulo 29 (actual Comité Europeo de Protección de Datos) que se informara al interesado cada vez que se recojan datos. Finalmente se alegaba que no concurrían agravantes en la actuación de la entidad y que, por tanto, se podrá imponer a lo sumo una mera sanción de advertencia o apercibimiento, pero en ningún caso de carácter económico. La Liga sostiene que cumplir con la medida que entiende adecuada la AEPD, como es mostrar en la pantalla del dispositivo la activación del micrófono y la geolocalización, puede afectar a la finalidad del tratamiento que no es otra que luchar contra el fraude en los derechos audiovisuales.

La Sala rechaza los argumentos y confirma el sentido de la resolución sancionadora, por cuanto hay existencia de tratamiento de datos personales, desde que se produce la captación de la información, pasando por la transformación, envío para su comparación y posterior recepción, se somete a tratamiento, al menos la siguiente información: el audio que se capta a través del micrófono, la dirección IP, un identificador de usuario, el sistema operativo y modelo de dispositivo, fecha y hora y ubicación. Asimismo, se envía la geolocalización cuando se produce la coincidencia de emisiones entre lo captado por el dispositivo y una emisión "legal". La Sala incide en que, si como indica La Liga, no se produce el tratamiento, no tiene sentido de que se informe acerca de él en la política de privacidad, ni menos aun solicitar el consentimiento del titular de los datos que supuestamente no va a tratar.

En cuanto a la transparencia, si bien durante la descarga de la aplicación en los dispositivos móviles se pedía el consentimiento para ambas funcionalidades -micrófono y geolocalización- y se informaba de ello en la política de privacidad, lo cierto es que, según la información ofrecida, estos se activaban a voluntad de La Liga siempre que ésta así lo estimara y que coincidiera con la emisión de partidos de futbol que organizaba. Lo cual ampliaba en gran medida las posibilidades de cuando se produciría dicha activación y sobre todo sin conocimiento exacto por parte del titular del dispositivo de cuando se producía ese tratamiento de datos. La entidad alegaba que ese aspecto ya había sido informado en la instalación de la aplicación, lo que la AEPD consideraba insuficiente para cumplir con el principio de transparencia, por lo que

reclamaba que se mostrará en la pantalla un aviso o icono que informara de que, en ese momento, se estaban captando el sonido y en su caso, la geolocalización. Respecto de este último dato, La Liga modificó su funcionamiento e insertó un icono cuando se activara dicha función, y no entiende el tribunal porque no hizo lo mismo respecto de la captación de sonidos, y precisamente esa falta de explicación priva de fundamento a las alegaciones de La Liga a este respecto.

Por todo ello confirma el criterio de la AEPD ya que resultaba necesario que, aun cuando en la política de privacidad de la aplicación y en la web, se informaba de los tratamientos analizados, y se otorgaba el consentimiento para los mismos, dada la injerencia que supone en el derecho a la protección de datos, se hacía necesario establecer mecanismos como la muestra de un aviso o icono en la pantalla, que permitiera al afectado conocer que en ese preciso momento se estaba captado el audio y en su caso, la geolocalización.

También en la resolución sancionadora se imputó inicialmente la infracción del artículo 7.3 del RGPD por cuanto para revocar el consentimiento prestado para activar ambas funcionalidades, no existía en la aplicación mecanismo alguno para llevar a cabo dicha revocación, sino que había que acudir al sistema operativo del dispositivo y configurar los permisos que se otorgaban a la aplicación. Lo que suponía una dificultad añadida en comparación para otorgar el consentimiento que si se podía hacer en la propia aplicación. Este mecanismo también se modificó durante la tramitación del procedimiento sancionador y no fue objeto de sanción.
La Sentencia se hace eco de estas cuestiones para demostrar, junto con otros elementos, que al contrario de lo manifestado por la recurrente, si se produjo instrucción en el procedimiento sancionador, pues entre otras cuestiones procedimentales, se alegó por ésta la vulneración de derechos procesales derivado de incluir en el acuerdo de inicio la determinación inicial de la sanción que pudiera corresponder en idénticos términos que se puesto de manifiesto cuando se ha citado anteriormente la Sentencia Audiencia Nacional de 9 de diciembre de 2022 que resuelve el Recurso nº 1994/2021.

En relación con la afección a otros principios, como el de exactitud, destaca una materia recurrente como es el tratamiento de datos personales en los sistemas de información crediticia o también conocidos coloquialmente como ficheros de morosos. La **Sentencia de la Audiencia Nacional de 1 de abril de 2022 que resuelve el Recurso nº 46/2020** interpuesto frente a la resolución sancionadora de la AEPD. Dicha resolución se basa en la vulneración del artículo 4.3 de la LOPD por la inclusión de los datos del afectado en un sistema de información crediticia sin que se haya requerido previamente de pago. Resolución que el tribunal considera conforme a Derecho al indicar que esta Sala necesariamente ha de confirmar el criterio de la Administración en el sentido de que los documentos aportados muestran el envío de mensajes de email, donde se alternan gestiones de recobro con peticiones de pago, ofrecimientos de pagos aplazados, incremento de la deuda pendiente con el paso de los días y cartas de inicio de demanda judicial. Más sin que prueben la notificación del requerimiento de pago previo a la inclusión de los datos del denunciante en el fichero de morosidad, con indicación del importe a pagar, plazo, forma y lugar y advertencia correspondiente, tal y como resulta obligado a tenor del referido artículo 38 del RLOPD en relación con los articulo 4.3 y 29 de la LOPD y según ha declarado esta Sala conforme a una reiterada y consolidada doctrina.

De donde se desprende que la anotación de los datos personales del afectado, en el fichero de solvencia patrimonial, en cuatro ocasiones, por parte de la entidad sancionada supone una vulneración de tal principio de calidad de datos. Infracción del artículo 4.3 LOPD de la que tal entidad actora debe responder, en cuanto responsable de la veracidad y calidad de los datos personales que suministra para su inclusión en ficheros de solvencia patrimonial y crédito. Por lo que tal vulneración del principio de calidad de datos ha de ser confirmada por la Sala.

Asimismo, en la Sentencia también se analizan las correspondientes alegaciones sobre la competencia de la AEPD por tratarse de una entidad británica sometida a otra normativa, recordando que esa cuestión que ya ha sido planteada por

la misma entidad recurrente a la misma Sala y Sección, que ha dictado sentencias con fecha de 21 de junio de 2019 (Recurso 342/2017) y de 13 de julio de 2021 (Rec.1233/19), entre otras, en las que hemos razonado lo siguiente:

(…) la Sentencia del Tribunal Supremo de 5 de febrero de 2019, estima el recurso de casación formulado contra la Sentencia de esta Sección de 25 de octubre de 2017 -recurso 99/2016-. Y llega a la conclusión que, resulta aplicable la LOPD, a una empresa domiciliada en un tercer Estado miembro de la Unión Europea, en concreto, en Luxemburgo, y que a los efectos de considerar que el tratamiento de datos se efectúa en el marco de las actividades de un establecimiento que se encuentre ubicado en territorio español, solo contaba para realizar su actividad en España con la utilización de un apartado de correos y la titularidad de una cuenta corriente, ya que había que tener en cuenta que la citada empresa "dirigía de forma regular actividades y operaciones a través de medios instrumentales radicados en España, adoptando decisiones relativas a los fines y medios del tratamiento de datos, al haberse acreditado que era la responsable de impartir las órdenes para que se incluyeran los datos personales del afectado en el fichero de solvencia patrimonial BADEXCUG".

Se añade que: "En este sentido, estimamos que la sentencia de instancia desconsidera la interpretación que del artículo 4.1.a) de la Directiva 45/96 ha efectuado el Tribunal de Justicia de la Unión Europea en la sentencia de 1 de octubre de 2015 (asunto C-230/14), en que se formula la directriz de que el concepto de establecimiento, a que se refiere dicha disposición, no puede entenderse en todo caso equivalente al de la sede social donde este registrada la sociedad responsable del tratamiento de datos, debiendo valorarse para la determinación de esta noción el grado de estabilidad de la instalación así como el grado de efectividad del desarrollo de la actividad y la naturaleza específica de las actividades económicas y de las prestaciones de servicios de que se trate.

Según se desprende de la mencionada sentencia del Tribunal de Justicia de la Unión Europea, cabe integrar en el concepto de establecimiento, desde una perspectiva funcional, las actividades que realice la empresa responsable del tratamiento de datos a través de un representante que disponga de los medios necesarios para la prestación de los servicios concretos de que se trate en el Estado miembro...".

Y llega el Tribunal Supremo a la siguiente interpretación del concepto de establecimiento del art. 2.1.a) de la LOPD: "A los efectos de considerar si es aplicable la normativa de protección de datos de carácter personal, de un Estado miembro de la Unión Europea a una empresa responsable del tratamiento de datos personales, en aquellos supuestos en que la sede principal esté ubicada en el territorio de otro Estado miembro de la Unión Europea, pero que realice actividades en otros Estados miembros, el concepto de establecimiento a que se refiere el artículo 2.1.a) de la Ley Orgánica 15/1999(…) 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".

En otro orden de cosas, procede citar la **Sentencia de la Audiencia Nacional de 18 de noviembre de 2022 que resuelve el Recurso nº 1439/2020** interpuesto frente a la resolución sancionadora, que tiene por objeto el análisis de la figura del Delegado de Protección de Datos (DPD) y los supuestos que requieren su designación y nombramiento.

Se trata de una conocida entidad cuyo objeto social consiste en el desarrollo y gestión de una plataforma tecnológica mediante la que a través de una aplicación móvil (APP) o de una web permite a determinadas tiendas locales de algunas ciudades en diferentes territorios ofertar o insertar sus productos y/o servicios a través de la misma y en su caso, si los usuarios de la APP y consumidores de las citadas tiendas locales así lo solicitan a través de la APP, de forma accesoria, intermedia en la entrega inmediata del producto.

La sanción analiza la ausencia de DPD al menos desde el año 2019 que es cuando se interponen las reclamaciones contra la entidad por dicha ausencia. La recurrente indica que su actividad de tratamiento está exenta de las obligaciones del articulo 37 RGPD y 34 LOPDGDD pero que contaba con un Comité de protección de datos con las funciones descritas en el artículo 39. Indica que su actividad principal no consiste en operaciones de tratamiento que requieran observación habitual y sistemática de interesados a gran escala. No obstante, nombró un DPD en enero del año 2020.

La Sala comienza indicando que la alegación referida a la existencia de un Comité de protección de datos y de un Subcomité no indica que exista el DPD, máxime cuando ni siquiera constaba su existencia en la web o se había comunicado a la AEPD que este Comité realizaba las funciones de DPD. Y en el art. 34 se establece la designación obligatoria de un DPD para los siguientes responsables o encargados y efectúa una enumeración que no debe considerarse como un número cerrado. Estamos ante un grupo empresarial que desarrolla una actividad a partir de una APP que, por su propia naturaleza, y además es notoriamente conocida, realiza constantes operaciones en las que intervienen particulares y en consecuencia y por la actividad que la entidad realiza accede a los datos personales de los usuarios, a su localización. El DPD es una figura obligatoria encargada de informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, debe velar por el cumplimiento normativo, y cooperar con la autoridad de control. Se escuda la recurrente en que disponía de un Comité de protección de datos que era un órgano suficiente para velar por el cumplimiento de la protección de datos y que se encontraba auxiliado por un subcomité. Y en principio debemos señalar que un DPD puede ser también una persona jurídica, o un órgano colegiado, pero es más que evidente que ese comité y subcomité con el que contaba la entidad era insuficiente para llevar a cabo las actuaciones exigidas al DPD puesto que nada más conocer de la reclamación procedió a su designación en forma comunicándolo a la AEPD.

En segundo término, recuerda los factores a tener en cuenta para estar ante un tratamiento de datos a gran escala según el Grupo de Trabajo del Articulo 29.

- El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente.
- El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento.
- La duración, o permanencia, de la actividad de tratamiento de datos.
- El alcance geográfico de la actividad de tratamiento, e indica que estamos ante una empresa cuya actividad principal es una intermediación entre los clientes y usuarios de la APP, que aportan sus datos personales para solicitar productos o servicios, y los propietarios de negocios que suministran esos productos u ofrecen esos servicios.

Esa actividad de intermediaria exige, necesariamente, que el usuario aporte sus datos personales y esos datos personales son seguidos de manera habitual y sistemática por parte de la actora puesto que estamos ante una APP popularísima cuyas técnicas para obtener datos, hacer un seguimiento de los mismos y predecir la geolocalización o ubicación de los interesados son factores que evidencian que se emplean los citados datos en actividades de mercadotecnia y por ello se exige que la empresa efectué un tratamiento de datos personales debiendo el encargado del tratamiento cumplir con absoluta plenitud las disposiciones del RGPD y LOPDGDD en el ejercicio de su actividad.

El GT29 hace referencia a las aplicaciones que son programas informáticos concebidos para un cometido concreto y dirigidos a un conjunto de dispositivos inteligentes. Y en este ámbito debemos incluir a la recurrente que se trata de una entidad a la que se puede acceder por cualquier usuario de un teléfono móvil, una tableta o una TV inteligente y como dice el GT29 el sistema operativo subyacente incluirá también

software o estructuras de datos que resultan importantes para servicios básicos de los dispositivos como, por ejemplo, el directorio de los teléfonos inteligentes, y la APP de esta entidad, que es una aplicación muy popular, puede recoger esos datos de los clientes, usuarios, de forma constante y continua, y de hecho una vez que el usuario emplea esta aplicación recibe información de ofertas, oportunidades, descuentos, de ahí que la entidad esté obligada a la adopción de cuantas medidas de seguridad sean necesarias ya que estamos ante una actividad a gran escala, concepto que la recurrente discute pero que el art. 91 RGPD acota y aunque no puede ser objeto de una determinación numérica o cuantitativa estricta precisamente porque los usuarios de apps tan populares como la recurrente son incontables, estamos ante un caso en que cualquier cantidad relevante puede poner en riesgo los datos de los usuarios que emplean la app, y siendo tantos los usuarios y por tanto los intereses afectados, éstos entran dentro de la categoría a gran escala y que si bien opera el término como un concepto jurídico indeterminado no puede la recurrente ampararse en ello cuando del riesgo de tratamiento de abundantes datos personales se está hablando.

Finalmente, en cuanto a las circunstancias agravantes en las que se basa la resolución sancionadora, la Sala indica que operan dos agravantes del art. 83.2 a) y g). respecto de la a) es evidente que el nº de afectados es multitud y, por consiguiente, sin mayor justificación que la que hemos ofrecido anteriormente referente a que la actividad de la actora es a gran escala queda demostrada la existencia de esta agravación. Y respecto de la g) se encuentren afectados identificadores personales básicos, igualmente es algo obvio. Datos tan personales como nombre, apellidos, domicilio, son datos cuyos tratamientos exigen las garantías necesarias de protección, que la actora está obligada a tratar y a proteger en garantía de preservar el derecho de las personas y su dirección privada de cualquier intromisión que se pueda producir por no adoptar las medidas necesarias de protección.

Sobre los principios integridad y confidencialidad relacionados con el de licitud, conviene citar la **Sentencia de la Audiencia Nacional de 10 de junio de 2022 que resuelve el Recurso nº 1684/2020** interpuesto frente a la resolución sancionadora de la AEPD que estima que una corporación local ha infringido lo dispuesto en los artículos 6.1 y 9 de la LOPD (normativa que resulta de aplicación en virtud de la disposición transitoria tercera de la LOPDGDD).

Los hechos declarados probados en la resolución recurrida se refieren, en síntesis, al acceso al ordenador de una empleada del ayuntamiento en el marco de un procedimiento disciplinario, dónde tenía documentación personal, sin que se limitara dicho acceso a la información relevante para el procedimiento disciplinario.

En el acuerdo de inicio del procedimiento disciplinario se hacía constar lo siguiente: ***al haber aparecido documentos en el escáner y la impresora que podrían suponer que la reclamante realiza actividades personales o profesionales dentro de la jornada de trabajo que nada tienen que ver con sus funciones de tesorera y que incluso podrían resultar incompatibles, mediante providencia de 26/02/2018, se ordenó al departamento de informática que investigue los documentos del ordenador personal de trabajo para aclarar esos hechos. De la inspección efectuada se obtuvieron varias carpetas de documentos personales sobre actividades privadas que se grabaron en un DVD".***

La trabajadora del ayuntamiento se enteró del acceso a su ordenador cuando se le notifica el 26 de febrero de 2018 el acuerdo de solicitud de incoación de expediente disciplinario. Los representantes de los trabajadores tampoco fueron advertidos de dicho acceso ni de los documentos "aparecidos en el escáner y en la impresora".

El contenido del DVD obtenido del ordenador de la trabajadora consistía en tres carpetas "mis documentos" y "download" con espacio de 1,7 GB. La vista de las tres carpetas revela que se contiene tanto información personal como profesional, copia de contrato de seguro de vehículo, declaración de hacienda, datos de contratos de préstamo hipotecario, o pago de bienes inmuebles, claves personales, datos bancarios, y de empresas como la franquicia Now Yow, cuenta de resultados Gestión Spa Hotel Myr, facturas de empresa de fotografía a nombre de otra persona, listado de cuentas anuales, pérdidas y ganancias del ejercicio 2017 de la empresa Aditivos Bio Energéticos y documentos sobre una sociedad que se dedica al negocio de una óptica.

No consta que el Ayuntamiento tuviera al momento del acceso al ordenador usado por la reclamante, el 26/2/18, una política y protocolo de uso del equipo informático de los empleados, prohibiciones o tipos de acceso permitidos, con advertencia sobre medios de control y consecuencias del mismo.

Sobre la vulneración del artículo 6 de la LOPD, el ayuntamiento sostiene que no es de aplicación la Sentencia Barbulescu pues se refiere a un conflicto laboral en el seno de una empresa privada y aquí nos encontramos ante una Administración Pública. Y en consecuencia no existe la expectativa de privacidad ya que se trata del uso de bienes públicos, escáneres, ordenadores e impresoras, sometidos al régimen del artículo 132 de la Constitución. Asimismo indica que el hallazgo de documentos en el escáner no fue el único motivo que le llevan a tener sospechas previas, que se trató de un hallazgo casual, que hizo necesario, junto con el incumplimiento reiterado de la jornada laboral y la presentación de un certificado de asistencia que no se ajustaba a la verdad, acceder al ordenador, tratándose de una medida necesaria y proporcionada. Por lo que su actuación estaría amparada en el artículo 6.1.c) y 6.1.e) del RGPD, en relación con el EBEP, el Real Decreto 128/2018, y la autonómica Ley 10/2010, de la Generalitat, sin que se haya infringido el artículo 6.1 de la LOPD.

La Sala rechaza los argumentos de la recurrente, indicando que en el ámbito público también se garantizan los derechos individuales de los empleados públicos, entre los que destaca el artículo 14. J bis) del EBEP que reconoce el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización (…) en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales. Además debe tenerse en cuenta el artículo 20.2 del mismo EBEP dispone que "Los sistemas evaluación del desempeño (…) se aplicarán sin menoscabo de los derechos de los empleados públicos" y el artículo 14.h) contempla entre dichos derechos, a la fecha de los hechos, el derecho al respeto de su intimidad y dignidad en el trabajo.

Añade que la legitimación para el tratamiento consistente en el acceso al equipo informático asignado a la reclamante puede obedecer a la comprobación del cumplimiento de sus funciones dentro de la relación que mantiene con el Ayuntamiento, y se puede arbitrar este tipo de accesos cuando se haya informado previamente del uso de los datos para dichos fines y en supuestos en que resulten proporcionales dichos accesos. Sin embargo, en el caso de autos no existía información previa sobre dicho uso o fines y tampoco existió proporcionalidad de la medida adoptada, pues se accede a todas las carpetas y archivos sin discriminar su contenido, de una forma especialmente invasiva, de tal forma que se han visto afectados documentos privados de la reclamante, documentos de salud, etc. que se han recogido de forma innecesaria y sin relación con lo que se buscaba.

Por tanto, se considera acreditada la infracción por vulneración del principio del consentimiento del artículo 6 LOPD, sin que nos hallemos ante ninguno de los supuestos habilitantes previstos en los incisos c) y e) del RGPD, invocados por la recurrente, pues no concurren ninguno de los

presupuestos establecidos en el artículo 8 de la LOPDGD para entender que se pueda considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos.

Sobre la vulneración del articulo 9.1 LOPD, se aduce que no se encuentra tipificada en el marco de la actual LOPDGDD en relación con el articulo 32.1 RGPD ya que no cita medidas de seguridad concretas, sino que se orienta a través del enfoque del riesgo. Por lo que debería haberse aplicado dicha norma al resultar más favorable.

La Sala rechaza tal argumento indicando que de acuerdo con los artículos 5.2 y 32.1 RGPD, se necesita un desenvolvimiento proactivo sobre la protección de los datos y guardar las evidencias de los pasos que se dan para cumplir con el RGPD junto a la circulación y vida de los datos, incluyendo eventuales instrucciones no solo de seguridad de soportes, sino como las que ha dictado para adaptarse al manejo de datos en sistemas de información y acceso del personal a los datos. De tal forma, que el hecho de que no se establezca expresamente como han de tratarse los soportes de almacenamientos de datos, no significa que no esté tipificado en el RGPD, y que deba reunir unos requisitos, y en ambos casos la conducta infractora acarrearía una infracción de medidas de seguridad en el tratamiento de datos.

En relación con los derechos previstos en los artículos 15 a 22 del RGPD deben diferenciarse aquellas que versan sobre el denominado Derecho al Olvido, de aquellas otras que tratan del resto de derechos.

Comenzando por estas últimas, se pone el acento en el modo o manera en que se ejercen los derechos ante el responsable, los supuestos que impiden su satisfacción, así como la necesidad de probar lo alegado respecto de los tratamientos sobre los que se solicita alguno de dichos derechos.

La **Sentencia de la Audiencia Nacional de 23 de diciembre de 2022 recaída en el Recurso nº 811/2019** interpuesto por un particular frente a la resolución de la AEPD que inadmite su reclamación por incumplimiento del derecho de acceso.

El recurrente en el año 2015 solicito a la subdelegación del Gobierno de Lugo, la cancelación/supresión de sus datos personales; este organismo, al comprobar que existían datos en el fichero de "sanciones administrativas". en septiembre de 2015, el Secretario General de la Subdelegación certificó que no disponían de ningún fichero de datos personales en los que consten los antecedentes a nombre de su persona.

Sostiene que sus datos siguen incorporados en dicho fichero, por lo que presentó una solicitud de cancelación ante la AEPD en el mes de octubre del año 2018.

La AEPD inadmitió la reclamación, y solicita la confirmación de dicha resolución por considerar que, respecto de la solicitud de supresión ante la Subdelegación del Gobierno de Lugo, ya se dio respuesta ese mismo año 2015, y que no consta otra solicitud durante el año 2018, por lo que solo en el caso en que ésta no atienda su reclamación en plazo podrá dirigirse a la AEPD.

Se pone de manifiesto que, para interponer una reclamación a la AEPD por desatención del derecho ejercido, primero se ha de dirigir ante el responsable del tratamiento en cuestión. No obstante, la Sentencia se inadmite el recurso por haberse interpuesto extemporáneamente.

La **Sentencia de 17 de junio de 2022 recaída en el Recurso nº 2007/202**1 tiene por objeto una resolución de archivo de la AEPD referida a una reclamación sobre el derecho de supresión.

El recurrente solicito a la compañía de le prestaba el servicio de telecomunicaciones la supresión de los datos relativos a la contraseña de acceso a su cuenta de correo electrónico así como la supresión de la conversación en la que la operadora le solicita dicho dato. La AEPD dio traslado a la compañía de telecomunicaciones y tras las alegaciones recibidas inadmitió la reclamación por considerar que no existía vulneración a la normativa de protección de datos, basándose en que la compañía mantenía los datos mínimos imprescindibles para prestar los servicios que se tenían contratados y para su facturación mientras siga siendo cliente el reclamante.

La Sala declara la inadmisibilidad del recurso contencioso por falta de legitimación al solicitar el recurrente la imposición de una sanción, no obstante, entra en el fondo del asunto confirmando el criterio de la AEPD referido a que no hay vulneración del derecho de supresión al haber informado al recurrente que no conservan más datos que los necesarios para prestar el servicio que tiene contratado. Con esta Sentencia se recuerda una de las circunstancias que impide la concesión de derecho de supresión.

Las **Sentencias de 3 de febrero de 2022 recaída en el Recurso nº 562/2020** y la de **26 de mayo de 2022 recaída en el Recurso nº 495/2020**, tienen por objeto el recurso de las resoluciones de la AEPD en las que se señala que el responsable del tratamiento a considerado que el derecho de acceso se ha contestado correctamente, y ha archivado las reclamaciones interpuestas por los afectados.

Los recurrentes aducen que las resoluciones no están suficientemente motivadas y que les causan indefensión. La Sala tras analizar la documentación obrante en autos y lo indicado en los artículos 12 y 15 del RGPD y 13 de la LOPDGDD, confirma el criterio de la AEPD, indicando que las resoluciones están motivadas, siendo cuestión diferente que los afectados no estén de acuerdo con los razonamientos que se dan, sobre los que en cualquier caso han podido alegar y probar lo que estimaran oportuno. Resultando inexistente la indefensión invocada.

Por su parte la Sentencia de la Audiencia Nacional de 20 de octubre de 2022 recaída en el Recurso nº 70/2021, aborda el derecho de supresión en relación con la respuesta que da el responsable del tratamiento frente a su ejercicio, y que la AEPD considera adecuada.

El reclamante ejerce su derecho de supresión frente a un Ayuntamiento contestando este que no están tratando sus datos. En desacuerdo con la contestación recibida interpone reclamación ante la AEPD que inadmite la misma por no aportar indicios suficientes de los que se derive una posible comisión de infracción a la normativa de protección de datos. En sede judicial insiste en que el Ayuntamiento no ha acreditado el borrado de sus datos, sin embargo, la Sala confirma el criterio de la AEPD indicando que éste no ha aportado ni en vía administrativa ni en este ámbito jurisdiccional, documentación alguna que desvirtúe lo afirmado en la respuesta que le proporciono la corporación local. En consecuencia, se desestima el recurso contencioso-administrativo confirmando la resolución de la AEPD.

Sobre el carácter repetitivo del ejercicio de las solicitudes, destaca la **Sentencia de la Audiencia Nacional de 1 de diciembre de 2022 recaída en el Recurso nº 152/2021**, contra la resolución de la AEPD, que considera como tal el ejercicio del derecho de acceso que realiza un interno en un Centro Penitenciario sobre el listado de los números de teléfonos autorizados en el sistema telefónico de llamadas y el listado con las personas autorizadas para visitarle, con el fin de gestionar las correspondientes rectificaciones. Según el demandante debería haber visto resuelta su solicitud con diligencia y “sin dilaciones indebidas”, y al no haberse actuado así, se vio obligado a reiterarla en diversas ocasiones unido al hecho de que fue trasladado de Centro Penitenciario.
La Sala confirma la resolución de la AEPD, indicando que al menos han sido dos las ocasiones en que se hizo entrega al demandante de la documentación que solicitó en forma de listados, llevada a cabo en el centro penitenciario, la más reciente el 17 de diciembre de 2018, y la más antigua en el otro Centro Penitenciario. Por lo que se contestó al derecho de acceso ejercitado. Asimismo, recuerda la aplicación de los artículos 12.5 del RGPD y 13.4 de la LOPDGDD referido a la posibilidad de negarse a actuar respecto de una solicitud cuando estas se consideren infundadas o excesivas y la consideración como tal cuando se realiza más de una en el plazo de seis meses, por lo que considera que la parte reclamada ha atendido el derecho de acceso de conformidad con la normativa de protección de datos.

Sobre el Derecho al Olvido, procede citar la **Sentencia de 17 de junio de 2022 recaída en el Recurso nº 140/2020**, frente a la resolución de la

AEPD que desestima la solicitud de supresión que realiza un particular frente al buscador titularidad de la compañía Google Inc.

Los hechos son que el que el reclamante ejercito su derecho de supresión ante Google LLC en relación con 18 URLs relacionadas en la solicitud, que muestran los datos personales de su padre fallecido como secretario judicial del Juzgado Militar de Prensa que condenó al poeta Miguel Hernández, para solicitar que el nombre de su padre no se asociara a las URLs reclamadas, invocando el artículo 3.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La solicitud no es atendida, por lo que se interpone reclamación ante la AEPD, que considera conforme a derecho la no concesión del derecho de supresión, en consecuencia, desestima la reclamación.

La Sala aborda en primer lugar, la circunstancia de que se está ejerciendo un derecho sobre los datos de una persona fallecida. Tras analizar el artículo 3 de la LOPDGDD y el Dictamen del Consejo de Estado de 26 de octubre de 2017 sobre la LOPDGDD, indica que los herederos y otras personas vinculadas al fallecido por razones familiares o de hecho, están facultados para ejercitar el derecho de supresión (derecho al olvido) regulado en el artículo 17 del RGPD, así como en el artículo 93 de la LOPDGDD sobre el derecho al olvido en las búsquedas de Internet, y en consecuencia, frente a lo sostenido por el representante de la Administración en la contestación, el recurrente está legitimado para ejercitar ante Google el derecho de supresión en relación con las URLS en cuestión que muestran los datos personales de su padre, ya fallecido, y solicitar que su nombre no se vincule a las citadas URLs.

De otro lado, no obsta a lo expuesto, el hecho de que la parte demandante pueda promover o haya promovido procesos civiles al amparo de la Ley Orgánica 1/1982, en relación con dichas URLs, al no haber incompatibilidad entre ambas vías de protección, como ha señalado esta Sala (SAN de 1 de octubre de 2008, Rec.1/2007). Criterio ratificado por el Tribunal Supremo, que en su Sentencia de 27 de septiembre de 2010 (Rec. 6511/2008) indica: "Tiene razón la sentencia recurrida al advertir el distinto objeto de los instrumentos que ofrecen la Ley Orgánica 1/1982 y la que regula el derecho a la protección de datos personales y la compatibilidad de entre unos y otros remedios".

Teniendo en cuenta lo anterior, resuelve el asunto indicando que las informaciones que nos ocupan revisten un interés público incuestionable al versar sobre la intervención del padre del recurrente, como secretario judicial del Juzgado Especial de Prensa que instruyó el procedimiento del poeta Miguel Hernández. Es decir, por la materia sobre la que versa la información, reviste una indudable relevancia pública habida cuenta la repercusión e interés de dicho procedimiento.

Las incorrecciones alegadas por el demandante, tales como que su padre fallecido en contra de lo que se decía, en esas fechas (1940) sí era licenciado en derecho y que no fue funcionario hasta 1944 cuando obtuvo plaza en la Administración Local, no afectan a la esencia de lo informado. Asimismo, de la prueba aportada con la demanda se ha constatado que el padre del recurrente no fue secretario del consejo de guerra que falló la sentencia de muerte, y así se ha reconocido por Google en la contestación. Sin embargo, la incorrección también alegada en la demanda, sobre el órgano exacto del que dicho Sr fue secretario judicial, no afecta tampoco a la esencia de lo informado, por cuanto su intervención como secretario judicial en el Juzgado Especial de Prensa que instruyó el sumario de Miguel Hernández, realizando diligencias de todo tipo, de instrucción e indagación, y dando fe de las actuaciones practicadas, ha quedado acreditada de la prueba documental aportada por la codemandada y en dichas publicaciones no se le atribuye un papel distinto del de secretario del órgano judicial.

Por otra parte, dichas informaciones se refieren a la vida profesional del padre del recurrente y no a su vida personal, circunstancia muy relevante para "modular" la intensidad que ha de merecer la protección del derecho regulado en el art. 18.4 de la Constitución, como ha señalado esta Sala en las Sentencias de 11 de mayo de 2017 (Rec.

30/2016), 6 de junio de 2017 (Rec. 1.797/2015), 14 de diciembre de 2018 (Rec. 520/2017), entre otras muchas, y así se destaca por la STS de 17 de septiembre de 2020 (Rec. 544/2019) que considera que esa distinción es trascendente en el juicio ponderativo de los intereses concurrentes.

El hecho de que el padre del recurrente, Alférez de Complemento honorífico del Cuerpo Jurídico Militar, no tuviera aprobada en aquellas fechas ninguna oposición y no fuera funcionario público, carece de la trascendencia que la parte pretende otorgarle , por cuanto lo relevante es que, por ser licenciado en Derecho, ejerció como secretario judicial del Juzgado Especial de Prensa que instruyó el sumario del encartado Miguel Hernández, y por esa razón y a los efectos ahora examinados de ponderar la relevancia del ejercicio del derecho de información y expresión, cabe entender que ejerció funciones públicas y en un asunto de indudable relevancia pública.

En cuanto el factor tiempo, el transcurso del tiempo no ha hecho decaer el interés que el asunto suscita, siendo prueba de ello su repercusión en los medios de comunicación en las fechas de interposición de la reclamación ante la AEPD en mayo de 2019. Además, cabe subrayar, en línea con la resolución recurrida y la STC 58/2018, la contribución sustancial que realizan las hemerotecas digitales a la preservación de noticias e informaciones que constituyen una fuente importante para la educación e investigación histórica y adquiere mayor relevancia para la valoración del legítimo interés público en el acceso a los archivos públicos cuando se trata de noticias a eventos pasados que sirven para la reescritura de la historia. Por todo lo cual y sopesadas todas las circunstancias del caso expuestas, como señala la citada STS de 11 de enero de 2019, en esta labor de ponderación de los derechos en juego, siempre desde la perspectiva del derecho a la protección de datos en que nos hallamos, y valorando el derecho de los internautas a informarse sobre tal cuestión, y que el derecho a la libertad de expresión comprende la crítica de la conducta de otro, aun cuando la misma sea desabrida y pueda molestar, inquietar o disgustar (SSTC 23/2010, de 27 de abril, y 9/2007, de 15 de enero), concluye que dichos enlaces estarían amparados por la libertad de información y de expresión (artículo 17.3.a) del RGPD, e incluso ciertos enlaces también por el apartado d) de dicho artículo 17.3, sin que proceda su supresión.

Respecto de los requisitos formales del ejercicio del derecho al olvido, destaca la **Sentencia de la Audiencia Nacional de 25 de octubre de 2022 recaída en el Recurso Nº 334/2021** contra la resolución de la AEPD que acuerdo proceder al archivo de la reclamación formulada por el recurrente contra Google Inc. por no haber atendido su derecho.

La resolución recurrida señala qué examinada la documentación obrante en la reclamación, se observa que el interesado solicita el derecho de supresión de todos sus datos personales en el buscador Google, sin especificar los enlaces que solicita que no sean indexados al realizar una consulta por su nombre. En concreto, solicita que "quiere ejercitar su derecho al olvido de todos sus datos personales que salen en el buscador GOOGLE. Lleva mucho tiempo intentando que esta supresión se lleve a cabo sin lograrlo". La Sala tras analizar las manifestaciones del recurrente y el artículo 93 de la LOPDGDD confirma la resolución de la AEPD al indicar que: Precepto que viene a incidir en que la identificación de los enlaces sobre los que se pretende ejercitar el derecho al olvido y de la información que afecta al interesado, constituye un presupuesto básico para poder efectuar el correspondiente juicio de ponderación de los intereses en juego. Así las cosas, resulta patente que la reclamación formulada ante la AEPD es completamente insuficiente en orden a efectuar la ponderación requerida por la Sentencia del TJUE de 13 de mayo de 2014, debiendo añadirse en esta línea, que si bien hay algunos procedimientos seguidos contra el recurrente en los que se ha declarado extinguida la responsabilidad penal por cosa juzgada y otros han sido sobreseídos provisionalmente, el propio recurrente reconoce en su reclamación que ha sido condenado en dos ocasiones, lo que requiere una individualización de los enlaces y de la información que contienen que corresponde efectuar al reclamante y que no ha hecho.

En el apartado relativo a la jurisprudencia del Tribunal Supremo, cabe citar la **Sentencia de 15 de febrero de 2022 que resuelve el Recurso de Casación nº 7359/2020**, interpuesto por una entidad frente a la Sentencia de la Audiencia Nacional de 22 de julio de 2019 (Recurso nº 136/2019) que confirma la resolución sancionadora de la AEPD por la vulneración del artículo 9 de la LOPD referido a las medidas de seguridad.

Los hechos por los que se sancionó a la empresa recurrente pueden sintetizarse en los siguientes: en las solicitudes de financiación de productos de telefonía clientes con la entidad figuraba una dirección de correo electrónico que no correspondía a los clientes-solicitantes, con la consecuencia de que se permitió el acceso no autorizado por parte de terceros, al menos a 14 solicitudes de financiación, en las que obraban datos personales de los clientes (nombre y apellidos, datos económicos, de domiciliación bancaria y firma). Es decir, el reclamante recibía en su correo electrónico las solicitudes de financiación de los clientes con los datos personales que se acaban de indicar.

El Auto por el que se admite el recurso de casación declara que es se suscita una cuestión que presenta interés casacional objetivo para la formación de la jurisprudencia, consiste en determinar si las infracciones de la Ley de Protección de Datos por fallos de las medidas de seguridad que puedan cometer los empleados de una persona jurídica, deben examinarse en atención al resultado y, por lo tanto, imputarse a la persona jurídica de la que dependa el empleado, con independencia de los medios y medidas de prevención que hubiera podido adoptar.

La entidad sancionada consideró que hubo un mal uso del formulario por parte de una de sus empleadas que, al rellenar la solicitud de financiación de algunos clientes, incluyó la dirección de correo electrónico del denunciante pensando que esa dirección era inexistente, al aludir a la provincia donde se ubica la tienda, para así poder dar curso al procedimiento de financiación, que exigía la introducción de una dirección de correo electrónico.

Pues bien, la Sala indica que "a obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento". Recuerda que en el caso de "obligaciones de resultado" existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad. En cambio, en las denominadas "obligaciones de medio", el compromiso adquirido es la adopción de medidas técnicas y organizativas, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia" o "de comportamiento".

La diferencia entre los citados conceptos radica en la responsabilidad en uno y otro caso. Mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada, en la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

Indica el Tribunal Supremo que tan solo resulta exigible a los responsables y encargados del tratamiento la adopción e implantación de medidas técnicas y organizativas que, conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Ahora bien, el Tribunal llega a la conclusión de que en el caso objeto del recurso, las medidas adoptadas por la entidad sancionada no fueron suficientes, ya que el programa utilizado no contenía ninguna medida de seguridad para comprobar si la dirección de correo electrónico era

real o ficticia y si correspondía a la persona cuyos datos estaban siendo tratados. Sostiene que el estado de la técnica en el momento de los hechos permitía establecer medidas para comprobar la veracidad de la dirección de correo electrónico.
Concluye que el hecho de que la filtración se produjera en última instancia por la actuación negligente de una empleada no exime a la empresa de su responsabilidad.

En consecuencia, fija la doctrina relativa al carácter de obligación de compromiso o actividad en cuanto a la seguridad en protección de datos, pero considera conforme a derecho la resolución de la AEPD.

En el ámbito de la justicia Constitucional, el Tribunal Constitucional dictó la **Sentencia de fecha 29 de junio de 2022 que resuelve el Recurso de Amparo nº 5310/2020** en el que el recurrente impugna las sentencias de las salas de lo contencioso-administrativo del Tribunal Supremo y de la Audiencia Nacional que anulan la resolución de la AEPD que insta a Google, Inc., para que adoptara las medidas necesarias a fin de que el nombre del solicitante no se asociara en los resultados de su motor de búsqueda a tres direcciones de páginas de internet. En consecuencia, a raíz de la Sentencia del Tribunal Supremo los datos personales seguirían apareciendo en dichos resultados, que es lo que se analiza en esta instancia constitucional.

Las publicaciones en internet hacen referencia a comentarios que se vierten sobre su persona en relación con su actividad de empresario inmobiliario.

El recurrente en amparo basa sus alegaciones en que los portales de quejas donde se publicó la información realizan un tratamiento ilícito de datos; que los órganos judiciales no han aplicado correctamente los criterios de relevancia pública de la información y del tiempo transcurrido en el juicio de ponderación de los derechos fundamentales afectados; y, finalmente, que se ha infringido el principio de preponderancia, debiendo también haberse aplicado el criterio de la veracidad a la información publicada.

El Alto Tribunal indica que la existencia del interés público puede venir dada porque el interesado afectado sea una persona pública o haya adquirido notoriedad pública y, en este segundo supuesto, la notoriedad pública puede haber sido alcanzada por la actividad profesional que desarrolla, o por difundir habitualmente hechos y acontecimientos de su vida privada, o puede haber adquirido un protagonismo circunstancial al verse implicado en hechos que son los que gozan de esa relevancia pública. También es posible que aun cuando el afectado no sea una persona pública ni haya adquirido notoriedad pública, pueda existir un interés del público en acceder a dicha información por referirse a una cuestión de interés general. En el caso analizado, indica que el recurrente

no adquirió ninguna notoriedad pública en el ejercicio de su actividad profesional al frente de las sociedades a través de las que desarrollaba su actividad de empresario inmobiliario.

Ahora bien, descartada la condición pública del recurrente debe determinarse si existe interés en acceder a la información por la materia de que se trate. El hecho de que la información tenga relación con la actual vida laboral del interesado es un elemento que tomar en cuenta, pero va a depender en gran medida de la naturaleza del trabajo mismo y del interés del público en tener acceso a esa información a través de una búsqueda por su nombre. Por eso, continua el Alto Tribunal, es necesario determinar, en primer término, si el acceso a lo publicado contribuye a la formación de una opinión pública libre, porque lo que merece especial protección constitucional es la difusión de ideas que colaboren a dicho fin y que faciliten que el ciudadano pueda formar libremente sus opiniones y participar de modo razonable en los asuntos públicos. Si existiese dicho interés, en cualquier caso, solo alcanzaría a aquella comunicación cuyo conocimiento sea necesario para que sea real la participación de los ciudadanos en la vida colectiva y que no sea formalmente vejatoria.

Los comentarios utilizados en los portales controvertidos, pese a descalificar al recurrente, no son formalmente vejatorios (límite a la prevalencia de la información). La ponderación exige atender al contexto en el que se producen las ideas y opiniones y valorar el contenido de las frases, su tono y su finalidad. En este caso se trata de los comentarios negativos de una usuaria sobre el servicio recibido por una de las sociedades en las que el recurrente es directivo, por lo que existe una finalidad crítica de esta empresa y de quienes la dirigen, y debe tomarse en cuenta que los descalificativos están influidos por su frustración personal de haber sido supuestamente estafada por dicha entidad. Adicionalmente, son comentarios que se contienen en una página de internet donde los usuarios intentan denunciar lo que consideran fraudes y estafas y estos se expresan libremente en un tono informal y con expresiones similares, siendo así que, efectivamente, en muchos portales de internet se utiliza un estilo coloquial, lo que al final reduce el impacto de las expresiones utilizadas. Por lo tanto, a la luz de dichas circunstancias, y en este específico contexto, no cabe calificar de desproporcionadas las expresiones controvertidas.

El problema radica más específicamente en determinar si la actividad profesional del recurrente –la promoción inmobiliaria–, junto a su papel desempeñado en la misma –a través de puestos directivos en empresas del sector–, genera un interés prevalente de los consumidores y usuarios en acceder a dichas publicaciones a través de un enlace en un motor de búsqueda.

No puede considerarse que la promoción inmobiliaria constituya una actividad profesional que dote de relevancia pública a cualquier publicación relativa a cualquier profesional de dicho sector y tampoco estamos ante una publicación que tenga carácter informador o periodístico, sino ante plataformas en las que los usuarios publican y denuncian lo que ellos consideran fraudes y lo hacen de forma anónima, como tampoco se está informando sobre hechos de relevancia penal en la medida en que las opiniones vertidas relatan una experiencia personal vivida con la empresa del recurrente, y el resultado de unas indagaciones personales realizadas. Asimismo, la aplicación del criterio de la relevancia pública debe ser más restrictivo cuando se trata de un acceso a través de un enlace en un buscador, en la medida en que aunque se suprima el enlace que se obtiene tras una búsqueda que tenga por objeto el nombre y apellidos de dicha persona, dicho acceso siempre podrá hacerse a través de la página web en la que está publicada la información original, o incluso a través del buscador tomando como objeto de búsqueda otros criterios distintos al nombre y apellido de la persona afectada. Por tanto, respecto de este elemento, el tribunal concluye que no puede concluirse que el acceso por dicho medio a meras opiniones y comentarios personales sobre la actividad profesional de personas particulares, que no son personas públicas ni han adquirido notoriedad por dicha actividad profesional, contribuya per se a la formación de una opinión pública libre.

En cuanto al factor tiempo, la sentencia recurrida indica que en las noticias posteriores al año 2010 no se habría disipado el interés de la información, en la medida en que hubo un reportaje en una televisión autonómica en el año 2012, otra noticia publicada en el año 2017 en un diario digital y cuatro publicaciones en un blog de un despacho de abogados que remitían a artículos de diarios ingleses, todos ellos en relación con un procedimiento penal en curso contra una de las empresas del recurrente, y sus ex directivos, esto es el recurrente. Sin embargo, el alto tribunal indica que dichas publicaciones no son pertinentes para sustentar la actualidad de las opiniones publicadas por la usuaria en los portales de quejas Las opiniones publicadas y que producen una injerencia en el derecho a la protección de datos personales, son un juicio subjetivo de una persona particular sobre la actividad profesional del recurrente, que relata, por una parte, el trato recibido durante su visita a España en la que un empleado de la empresa, de la que aquel era directivo, le enseñó determinadas propiedades, y, por otro lado, comparte que al volver de España llevó a cabo una investigación en la que había descubierto que el recurrente había dejado su empresa anterior «con una estela de problemas», y que era «un gran tirano que trata a sus empleados como esclavos. Es decir, en ninguno de ellos se hacía alusión alguna a las informaciones contenidas en las noticias que se han tenido en cuenta por las resoluciones judiciales para sustentar la actualidad de las opiniones publicadas que se refieren a un procedimiento judicial penal en el que está supuestamente incurso el recurrente en amparo. Si bien dichas noticias sobre ese procedimiento penal pueden ser actuales, y, en consecuencia, pueden justificar un interés superior del público en acceder a las mismas, la actualidad no se traslada a las opiniones vertidas sobre el recurrente en los portales de quejas que no tienen por objeto esas diligencias penales. Por tanto, los elementos tomados en consideración por las sentencias impugnadas no ponen de manifiesto la existencia de un interés preponderante del público en acceder a dicha información, al extremo de permitir sacrificar el derecho al olvido del recurrente respecto al motor de búsqueda Google.

En consecuencia, al haber anulado la resolución de la AEPD se ha vulnerado el derecho fundamental a la protección de datos. Por todo ello estiman el recurso de amparo.

Finalmente, en el ámbito europeo, el Tribunal de Justicia de la Unión Europea ha dictado, entre otras, las siguientes sentencias:

La **STJUE de 1 de agosto de 2022, Asunto C-184/2020** analiza la obligación de publicar información personal de empleados públicos para cumplir con la normativa que regula la lucha contra la corrupción y conflictos de intereses.

El afectado ocupa un cargo directivo en una entidad pública de Lituania en el ámbito de la protección medioambiental, y la Comisión Superior que se ocupa de aplicar la ley sobre conciliación de intereses de Lituania, le requirió para que presentara la declaración de intereses prevista en dicha norma y al no presentarla declaró la comisión de la correspondiente infracción.

Debe tenerse en cuenta que la declaración de intereses se publica en internet, en la página web del citado organismo y puede contener información no sólo del declarante sino de terceros, como por ejemplo el cónyuge o pareja de hecho.

La Sentencia analiza si la publicación en internet de la citada declaración es conforme a la normativa de protección de datos, para lo que en primer lugar, establece que en la medida en que está prevista en el Derecho Lituano como obligación de que la citada Comisión publique en su página web las declaraciones, constituye un tratamiento basado en el artículo 6.1 c) del RGPD, señalando también que velar por que los responsables de la toma de decisiones en el sector público ejerzan sus funciones con imparcialidad y objetividad y evitar que sean influidos por consideraciones que tengan que ver con intereses privados son acciones dirigidas a garantizar una buena gestión de los asuntos públicos y de los bienes públicos y la lucha contra la corrupción constituye un objetivo al que los Estados miembros se han adherido tanto a escala internacional como a escala de la Unión.

Ahora bien, también realiza el juicio de proporcionalidad, indicando que si bien dicha medida puede resultar idónea para incentivar la actuación de imparcialidad, en lo que se refiere a la necesidad, indica que hay en la norma Lituana otras medidas que permitirían alcanzar el mismo fin sin los efectos que tiene la publicación en internet de dicha información, pues también se cumpliría con la comunicación de dicha declaración a la Comisión Superior que es la encargada de controlar y supervisar el cumplimiento de la norma. Frente a esto la citada Comisión indica que no dispone de recursos humanos suficientes para controlar de modo eficaz todas las declaraciones que le son presentadas. Sin embargo, el Tribunal Europeo indica que la falta de asignación de recursos a las autoridades públicas no puede constituir, en ningún caso, un motivo legítimo que pueda justificar un menoscabo de los derechos fundamentales garantizados por la Carta.

Indica que a los efectos de apreciar la proporcionalidad del tratamiento objeto del litigio principal, conviene medir la gravedad de la injerencia en los derechos fundamentales a la intimidad y a la protección de datos personales que este tratamiento supone y comprobar si la importancia del objetivo de interés general perseguido por este está en consonancia con la referida gravedad.
Con objeto de evaluar la gravedad de esta injerencia, debe tenerse en cuenta, en particular, la naturaleza de los datos personales en cuestión, en particular el carácter potencialmente sensible de los mismos, así como la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos y el modo en que acceden (sentencia de 11de diciembre de 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064,apartado 57).

Señala que ha de destacarse, por un lado, que la divulgación pública, en Internet, de datos nominales relativos al cónyuge, compañero sentimental o pareja del declarante o a las personas allegadas o conocidas por este que puedan dar lugar a un conflicto de intereses, así como la mención del objeto de las operaciones económicas cuyo valor supere los 3 000 euros pueden revelar información sobre algunos aspectos sensibles de la vida privada de las personas afectadas, entre ellos, por ejemplo, su orientación sexual. Además, en la medida en que contempla una divulgación pública de esa naturaleza de datos nominales relativos a personas distintas del declarante —en su condición de responsable de la toma de decisiones en el sector público—, el tratamiento de los datos personales previsto en la norma Lituana también afecta a personas que carecen de tal condición y respecto de las cuales los objetivos perseguidos por esa norma no se imponen del mismo modo que respecto al declarante.

La gravedad de esa injerencia puede aumentar más aún por el efecto acumulativo de los datos personales que son objeto de una publicación como la que tiene lugar en el litigio principal, dado que combinación permite hacer un retrato particularmente detallado de la vida privada de las personas afectadas [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017,EU:C:2017:592, apartado 128].

En consecuencia, dicho tratamiento puede llegar a facilitar el libre acceso a esos datos por parte de personas que, por razones ajenas al objetivo de interés general de prevención de los conflictos de intereses y de la corrupción en el sector público, pretendan informarse sobre la situación personal, material y económica del declarante y de los miembros de su familia.

Considera el Tribunal Europeo que estamos ante una injerencia grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de las personas afectadas. Incide en que ha de señalarse que la publicación en línea de la mayor parte de los datos personales contenidos en la declaración de intereses privados de todo directivo de un establecimiento que reciba fondos públicos, como la que es objeto del litigio principal, no cumple los requisitos de ponderación equilibrada. En efecto, en comparación con una obligación de declaración a la que se une el control de su contenido por parte de la Comisión Superior, control por cuya efectividad debe velar el Estado miembro de que se trate dotando al referido órgano de los recursos

necesarios al efecto, dicha publicación representa un menoscabo considerablemente más grave de los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta, sin que esta mayor gravedad pueda compensarse con los eventuales beneficios que pudiera suponer la publicación de todos esos datos para prevenir los conflictos de intereses y luchar contra la corrupción. Además, de ningún elemento de los autos se desprende que la legislación nacional aplicable al litigio principal haya establecido garantías contra riesgos de abusos a los que se ha hecho referencia.

Por tanto, considera la publicación de la declaración de intereses en la página web de la Comisión Superior contraria a Derecho.

En segundo término, aborda si se están afectados categorías especiales de datos en la referida declaración de intereses privados, analizando la posible divulgación indirecta que puede suceder. Resuelve el asunto indicando que aun cuando estemos ante divulgación "indirecta" dicho tratamiento no queda fuera del régimen de protección reforzado establecido por las mencionadas disposiciones, pues de quedar fuera se menoscabaría el efecto útil de ese régimen y la protección de las libertades y de los derechos fundamentales de las personas físicas que pretende garantizar.

Por otra parte la **STJUE de 28 de abril de 2022, Asunto C-319/2020** aborda la legitimación de las asociaciones de consumidores y usuarios para interponer reclamaciones en materia de protección de datos mandato y con independencia de la vulneración de derechos concretos de un interesado y derivado del incumplimiento de la normativa de defensa de la competencia.

El Tribunal considera que es conforme al artículo 80.2 del RGPD que una asociación de defensa de los intereses de los consumidores pueda ejercitar acciones judiciales sin mandato conferido a tal fin y con independencia de la vulneración de derechos concretos de los interesados, contra un presunto infractor de la normativa de protección de datos personales, invocando el incumplimiento de la prohibición de prácticas comerciales desleales, de una ley en materia de protección de los consumidores o de la prohibición del uso de condiciones generales nulas, toda vez que el tratamiento de los datos de que se trate pueda afectar a los derechos que el RGPD confiere a personas físicas identificadas o identificables.

Finalmente indicar la **STJUE de 20 de Octubre de 2022, Asunto C-77/2021**, analiza los principios de limitación de finalidad y limitación del plazo de conservación en relación con la creación y mantenimiento de una base de datos por parte de un operador de telecomunicaciones, creada para realizar pruebas y corregir errores, a partir de los datos personales previamente recogidos y conservados en otra base datos referida a los clientes de la entidad.

Indica la Sentencia que la recogida de los datos de la base a partir de la que se crea la otra, responden a la finalidad de celebración y ejecución de contratos de abono por parte de la entidad con sus clientes, de conformidad con el artículo 6.1 b) RGPD. Asimismo, el hecho de que el responsable del tratamiento registre y conserve, en una base de datos de nueva creación, datos personales que conservaba en otra base de datos constituye un «tratamiento ulterior» de esos datos.

En cuanto a la compatibilidad, indica que de una lectura conjunta de los artículos 5.1 b) y 6.1 a) y 4 del RGPD, se desprende que la cuestión relativa a la compatibilidad del tratamiento ulterior de datos personales con los fines para los que estos se hayan recogido inicialmente solo se plantea en el supuesto de que los fines del tratamiento ulterior no sean idénticos a los fines de la recogida inicial.

Para lo que cita el test de compatibilidad del articulo 6.4 RGPD y señala que dichos criterios reflejan la necesidad de que exista una relación concreta, lógica y suficientemente estrecha entre los fines de la recogida inicial de los datos personales y su tratamiento ulterior, y permiten asegurarse de que el tratamiento ulterior no se aparte de las expectativas legítimas de los abonados en cuanto a la utilización ulterior de sus datos. Dichos criterios permiten delimitar la reutilización de datos personales recogidos previamente,

garantizando un equilibrio entre, por un lado, la necesidad de previsibilidad y de seguridad jurídica respecto de los fines del tratamiento de datos personales recogidos previamente y, por otro, el reconocimiento de cierta flexibilidad al responsable del tratamiento para gestionar estos datos, y contribuyen de este modo a la realización del objetivo de garantizar un nivel uniforme y elevado de protección de las personas físicas.

La realización de pruebas y la corrección de errores que afectan a la base de datos de los abonados guardan una relación concreta con la ejecución de los contratos de abono de clientes particulares, en la medida en que tales errores pueden resultar perjudiciales para la prestación del servicio previsto contractualmente y a cuyo fin se recogieron inicialmente los datos. un tratamiento de este tipo no se aparta de las expectativas legítimas de los clientes en cuanto a la utilización ulterior de sus datos personales. Por lo que considera que podemos estar ante finalidades compatibles. Y en cuanto a la conservación de los datos en la base de datos creada ulteriormente, señala que únicamente podrán almacenarse mientras cumplan la finalidad de corregir errores, es decir, no pueden almacenarse en un periodo superior al necesario para la realización de las pruebas oportunas.

2.3. Tecnológicos

La División de Innovación Tecnológica (DIT) se crea a principios del año 2016 formando parte de la Unidad de Apoyo de la Dirección. El objeto era disponer de una unidad que diera soporte a responsables, encargados y DPD para la aplicación del principio de Responsabilidad Proactiva del Reglamento General de Protección de Datos (RGPD) y estudiase el estado del arte de los nuevos tratamientos de datos que involucraban el uso de tecnologías disruptivas.

En el RD 389/2021, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, la DIT viene depender directamente de la Presidencia de la AEPD asumiendo las siguientes competencias:

- Asesorar a la dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos de carácter personal. Analizar las implicaciones y alternativas del estado de arte de la tecnología y generar el conocimiento necesario para anticiparse a los cambios de la misma.

- Impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos. Este punto incluye el desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos y la elaboración de guías que impulsen el cumplimiento de aspectos específicos del principio de responsabilidad activa del Reglamento (UE) 2016/679 en el ámbito tecnológico, según su artículo 57.1. b) y d).

- Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del Reglamento (UE) 2016/679; en particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.

- Gestionar el Registro de brechas de seguridad para facilitar a los responsables el cumplimiento de lo previsto en el artículo 33 del Reglamento (UE) 2016/679. Analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la dirección la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción.

- Emitir informes, recomendaciones y dictámenes sobre las consultas previas relativas a la Evaluación de Impacto para Protección de Datos realizadas por los responsables conforme al artículo 36 del Reglamento (UE) 2016/679, en virtud de lo previsto en su artículo 57.1.l).

- La elaboración de una lista positiva y, en su caso, otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k del Reglamento (UE) 2016/679.

Las actividades más destacadas de la DIT durante el año 2022 se describen a continuación:

2.3.1.Elaboración de guías y modelos, estudios y notas técnicas

Buena parte de las áreas de actividad en las que se encuentra implicada la DIT es la elaboración de guías, modelos, estudios y notas técnicas en las que se vierten recomendaciones de carácter técnico con relación a actividades concretas en las que existe un tratamiento de datos personales. Varias han sido las áreas que han sido objeto de análisis a lo largo de 2021, incrementando el contenido técnico del blog de la AEPD y el área de innovación y tecnología con las siguientes publicaciones y herramientas desde el 1 de enero al 31 de diciembre de 2022:

- Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de una consulta previa

- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas

- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado

- Neurodatos y neurotecnología: privacidad y protección de datos personales

- Metaverso y privacidad

- Dark patterns: Manipulación en los servicios de Internet

- Informe sobre la Acción Coordinada CEF sobre el uso de servicios en la nube por parte de organismos públicos

- Informes Nacionales sobre dicha Acción Coordinada CEF

- Mapa de referencia para tratamientos que incluyen Inteligencia Artificial

- Privacidad desde el diseño: Computación segura multi-parte, compartición aditiva de secretos

- 10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)

- Hoja de ruta para garantizar la conformidad con la normativa de protección de datos

- Infografía para la Comunicación de Brechas de Datos Personales

- Herramienta para evaluar la obligación de notificar a la Autoridad de Control: ASESORA-BRECHA

- Herramienta EVALÚA-RIESGO en su segunda versión para entorno web

- Blockchain (III): Smart contracts y datos personales

- Brechas de datos personales: entornos de desarrollo y preproducción

- Sin privacidad no hay ciberseguridad

Otros documentos en los que ha participado la DIT como co-ponente son:

- ENISA: 'La adopción de técnicas de seudonimización. El caso del sector sanitario'

- ENISA: Ingeniería de la protección de datos
- PDPC SINGAPURE: Guía Básica de Anonimización, versión en español
- PDPC SINGAPURE: Herramienta básica de Anonimización, versión en español
- EDPS: TechDispatch 1/2022 Redes Sociales Federadas
- EDPB: Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them

Con relación a los contenidos desarrollados por la DIT se muestran a continuación algunas de las cifras de descargas más significativas que reflejan las principales inquietudes de los responsables y encargados de los tratamientos de datos personales con relación al principio de responsabilidad activa. En la siguiente tabla se muestran aquellos documentos de ayuda que han superado las 10.000 descargas durante el 2022:

Contenidos desarrollados por la DIT	Descargas
Guía para la gestión y notificación de brechas de seguridad	52.416
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	45.478
El uso de las tecnologías en la lucha contra el COVID19	36.298
Guía de Privacidad y Seguridad en Internet	34.062
Cuándo y cómo se debe comunicar una brecha de datos a los afectados	25.225
14 equívocos con relación a la identificación y autenticación biométrica	24.039
Guía de Protección de Datos por Defecto	21.701
Hoja de ruta para garantizar la conformidad con la normativa de protección de datos	20.312
Mapa de referencia para tratamientos que incluyen Inteligencia Artificial	19.975
Guía de Privacidad desde el diseño	19.911
Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo	19.162
Orientaciones y Garantías en los procedimientos de anonimización	19.089
Drones y Protección de Datos	13.570
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial	12.387
Guía de Tecnologías y Protección de Datos en las AA.PP.	11.652
Introducción al hash como técnica de seudonimización de datos personales	10.091

Como puede observarse, la suma de las descargas de dichos documentos alcanza un total de más de 400.000 descargas que, sumadas al resto de documentos que no superan el total de las 10.000 descargas durante el 2022, alcanzan un total de más de 500.000 descargas, lo que pone de manifiesto el gran interés de responsables y encargados de los tratamientos de datos personales así como de los desarrolladores de productos o, incluso, de otras Autoridades de Control por los contenidos que ha producido la DIT desde 2016.

2.3.2.Notificaciones de brechas de datos personales

Con relación a la misión de gestión, análisis y evaluación de las brechas de datos personales, se han realizado las siguientes actividades:

- 1751 notificaciones de brechas de datos personales se han gestionado durante este periodo dando lugar a diez traslados a la Subdirección General de Inspección de Datos para una segunda evaluación. Por otra parte, estas brechas han generado un total de 31 requerimientos a los responsables para que cumplieran con su obligación de comunicar a los interesados tal y como exige el artículo 34 del RGPD.

- Publicación la herramienta para asesorar al responsable en su obligación de notificar a la Autoridad de Control de acuerdo con lo previsto en el artículo 33 del RGPD, la anteriormente mencionada herramienta ASESORA-BRECHA.

- Actualización de la herramienta en background para una gestión más racional de las brechas notificadas a la AEPD para su adecuación al formulario actualizado en 2021.

Otras tareas relacionadas con la gestión de brechas de datos personales son:

- Mantenimiento de la sección sobre brechas de datos personales con, entre otros, la publicación en la página web de la AEPD de los informes mensuales sobre brechas notificadas a la AEPD con un análisis sobre su tipología, además de agrupar todo el material de interés sobre brechas de datos personales.

- Mantenimiento del canal de notificaciones de brechas de datos personales de la Sede Electrónica de la AEPD.

2.3.3.Evaluaciones de impacto y consultas previas

Con relación a las tareas relativas al análisis de las consultas previas relativas a la Evaluación de Impacto para Protección de Datos, las actividades han sido las siguientes:

- En el periodo del informe se han remitido a la AEPD y gestionado un total de 6 solicitudes de consulta previa.

- Puesta en producción de la herramienta para la gestión de consultas previas.

La DIT presta también asesoramiento técnico al canal del DPD participando en aquellas consultas que se reciben o elaborando la respuesta a las mismas, durante el periodo de este informe han sido elaboradas un total de 6 respuestas a las consultas recibidas.

Con carácter general, el número de consultas previas recibido, y la calidad de las evaluaciones de impacto en protección de datos realizadas por los responsables, continúa evidenciando una interpretación de los requisitos que exigen los artículos 35 y 36 del RGPD meramente formal sin dar respuesta al enfoque de riesgos que exige el principio de responsabilidad activa del RGPD y sin atender a la metodología de gestión de riesgo planteada en la guía de *Gestión del Riesgo y Evaluación de Impacto relativa a la protección de datos* y, en consecuencia, sin atender los requisitos de la Instrucción 1/2021, dando una interpretación del riesgo centrada en el cumplimiento normativo y no en los riesgos que los tratamientos de datos

personales implican para los interesados. En este sentido se pone de manifiesto, además de la no adecuación a los requisitos exigidos en la Instrucción 1/2021 sobre la función consultiva de la AEPD, la dificultad de los responsables y sus DPD a la hora de entender la obligación de llevar a cabo el análisis de necesidad y proporcionalidad de los tratamientos que se plantean así como la dificultad de entender el levantamiento de la prohibición del artículo 9.2 del RGPD que, con frecuencia, se viene a confundir con las bases jurídicas del tratamiento.

El RGPD hace alusión al término riesgo en numerosas ocasiones (artículos 4.24, 23.2.g, 24.1, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 39.2, 49.1, entre otros) riesgos que, en su conjunto, necesariamente deben identificarse y evaluarse en el marco adecuado para su gestión que previamente debe de haberse establecido. La gestión del riesgo es una disciplina que constituye uno de los pilares de la gestión de cualquier organización y, en ningún caso, la gestión del riesgo para los derechos y libertades de las personas físicas debe contemplarse como un elemento aislado del resto de procesos de una organización sino como un elemento más a gestionar de manera global por los responsables. Interpretar que el riesgo en materia de protección de datos, para dar respuesta a los requisitos que exige el RGPD, no debe limitarse a un simple ejercicio de checkbox limitado un modelo de cumplimiento formal de las obligaciones de la normativa de protección de datos y es contrario al espíritu al working paper 218 *(WP218)* relativo a la Declaración sobre el papel de un enfoque basado en el riesgo en el marco legal de la protección de datos y contrario al propio espíritu del RGPD.

Sin embargo, como se ha señalado, este no es el único malentendido en la aplicación del RGPD, con frecuencia el principio de proporcionalidad se confunde con el principio de minimización de datos lejos de lo que señala el considerando 4 del RGPD, del mismo modo también el principio de necesidad del tratamiento se viene a reducir al análisis de necesidad de llevar a cabo la EIPD frente a la necesidad a la que el propio tratamiento, en sus finalidades, tendría como objetivos dando respuesta a un adecuado balance riesgo-beneficio que dicho tratamiento pudiera tener para los interesados.

Desde la DIT se han impulsado las iniciativas necesarias para dotar a responsables y encargados de recursos de ayuda a fin de paliar las deficiencias y errores de interpretación que han venido observando desde la entrada en vigor del RGPD, publicando en 2021, la nueva *Guía de análisis de riesgos y evaluaciones de impacto en protección de datos*, además de la herramienta *Evalúa-Riesgo* (actualizada a formato web en 2022) junto con un documento de *tablas* o anexos que permite a los responsables abordar los retos planteados por el RGPD para dar respuesta a las obligaciones que el RGPD establece en su enfoque de riesgos.

Otro de los problemas observados es la entrada en la AEPD de consultas previas por canales distintos al canal de consultas previas de la sede electrónica, debe de tenerse en cuenta que los plazos señalados en el artículo 36 del RGPD son muy limitados y la entrada de consultas previas por canales externos al canal de consultas previas implica una gestión adicional de cada consulta que reduce considerablemente los plazos desde el punto de vista material. En este sentido, la Instrucción 1/2021, en general, vino a plantear requisitos mínimos a tener en cuenta con relación a la evaluación de impacto que debe de acompañar a la solicitud de consulta previa además de incluir la exigencia de utilizar el canal de consultas previas, evitando así, demoras innecesarias que reduzcan materialmente los plazos de respuesta.

2.3.4. Cooperación con asociaciones y otras entidades

Con el propósito de impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos, la DIT viene colaborando en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promoviendo la colaboración con las Universidades con el fin de impulsar la

protección de datos a fin de generar el conocimiento necesario para anticiparse a los cambios de la tecnología, en este sentido se han establecido las siguientes colaboraciones con:

- Autoridades Autonómicas de Protección de Datos en aspectos tecnológicos.
- Secretaría General de Administración Digital, (SGAD) en consultas sobre temas de regulación tecnológica.
- Secretaría de Estado de Digitalización e Inteligencia Artificial, a la que se han atendido sus consultas sobre temas tecnológicos con trascendencia en protección de datos.
- INCIBE, con relación a la coordinación en la comunicación de brecha de seguridad
- Consejo Superior de Investigaciones Científicas (CSIC), en la revisión de guías y notas técnicas
- Centro para el Desarrollo Tecnológica e Industrial (CDTI) Comisión del seguimiento del Convenio de Colaboración y en la revisión de guías.
- Comité Técnico de Normalización CTN-71 sobre Tecnologías Habilitadoras Digitales y en el Subcomité Técnico SC42 sobre Inteligencia Artificial y Big Data, como vocales.
- Universidad Carlos III-IMDE A Networks en temas de consultas tecnológicas.
- Universidad de Alcalá de Henares en el marco de una extensión del proyecto para estudiar técnicas de gobernanza en Blockchain y propuesta de elaboración de un convenio de colaboración.
- Universidad Nacional de Educación a Distancia (UNED), en la revisión de guías y como miembros del Advisory Board proyecto UNED Forensic GDPR.
- Universidad Rey Juan Carlos: colaboración en temas de tratamientos biométricos.
- Fundación Éticas: colaboración el desarrollo de guías de auditorías de aplicaciones de Inteligencia Artificial
- Grupo OdiseIA, en colaboración en temas de Inteligencia Artificial.
- Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC), en la revisión de guías.
- Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI) en la revisión de guías.
- Asociación Women in a Legal Word, en la revisión de guías y preparación de un Protocolo de Colaboración.
- Observatorio de Bioética y Derecho-Cátedra UNESCO de Bioética. Universidad de Barcelona, en la preparación de un Protocolo de Colaboración.

En relación con la participación en iniciativas internacionales de carácter tecnológico en protección de datos, las acciones más reseñables son las siguientes:

- Participación en el Subgrupo de Tecnología del Comité Europeo de Protección de Datos, entre otras cosas, participando como co-revisores en la guía de Blockchain y la guía de anonimización (pendientes de publicar), presentando la iniciativa AppCensus de IMDEA, o colaborando en la acción coordinada CEF sobre cloud computing en las Administraciones Públicas.
- Colaboración con el Supervisor Europeo de Protección de Datos, que se ha materializado en la publicación en común de una nota sobre equívocos en biometría y se está trabajando

en una herramienta conjunta de análisis de cookies.

- Definición del Componente 5 (Protección de Datos) del proyecto Twinning EU Support to E-Governance and digital economy in Ukraine y asunción del rol de Component Leader del proyecto.

- Participación en el grupo de Inteligencia Artificial de la Conferencia Internacional de Autoridades.

- Colaboración con la Universidad de las Naciones Unidas en el campo de Blockchain, con la que se ha firmado un nuevo MOU de colaboración

- Colaboración con la Red Iberoamericana como revisores de los documentos publicados sobre Cloud Computing.

- Colaboración con la Autoridad Brasileña de Protección de Datos, con la que se ha firmado un MOU de colaboración.

- Colaboración con la Escuela Politécnica Federal de Lausana, a través de la científica Carmela Troncoso, en la elaboración conjunta sobre la nota técnica "Recomendaciones para el despliegue de aplicaciones móviles para el control del acceso a espacios públicos".

- Asesoramiento a la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP) en proyectos internacionales de protección de datos.

Finalmente, colaboración con la División Internacional en la participación española en acciones puntuales internacionales.

En cuanto a la obligación de asesorar a la Dirección de la AEPD, así como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos, desde su creación la DIT participa de forma regular en las actividades e iniciativas de la AEPD.

Tales actividades son muy numerosas y listarlas sería prolijo, por lo que se destaca:

- Participación de miembros de la DIT como ponentes en diversos foros internacionales, como el BvD DPO Spring Congress 2022 en Alemania, el euLISA Webinar Privacy and data protection by design, o el Seminario RIPD 2022 (webinario) sobre Protección de datos ante la disrupción tecnológica: Computación en Nube e Inteligencia Artificial.

- Participación de miembros de la DIT como ponentes en diversos foros realizados en España con ámbito internacional y nacional, como II CONGRESO INTERNACIONAL: "Dinero Digital y Gobernanza TIC en la UE: nuevos estándares jurídicos y tecnológicos" de la Universidad de Alicante, II Jornada Protección de Datos Personales IAPP-UFV, Jornadas de Digitalización del Consello Económico e Social de Galicia, II Congreso Internacional "Dinero Digital y Gobernanza TIC en la UE" o ponencias en el curso de la UIMP "Privacidad Innovación e Igualdad".

- Otra formación dirigida a otras instituciones y administraciones públicas (AECID, Ministerio de Justicia, de Inclusión, de Universidad, de Transporte, de Educación, de Política Territorial, Ayuntamiento de Madrid, etc.)

En cuanto a la formación interna, la DIT ha impartido:

- Curso interno introductorio al análisis de aplicaciones móviles (4h.)
- Curso interno sobre cookies (4h.)
- Curso interno sobre responsabilidad proactiva (12 h.)
- Curso interno sobre criptografía y privacidad (16h.)
- Curso interno de formación en el RGPD impartido a través de la plataforma del INAP a distintos Ministerios.

- Realización de un videotutorial práctico sobre herramientas de la AEPD para el tercer sector

- Desde la DIT se viene dando soporte al canal del DPD con relación a las consultas de índole técnica de los responsables, en general consultas relacionadas con aspectos sobre evaluaciones de impacto, análisis de riesgos, medidas de seguridad, tecnologías, tratamientos biométricos, notificaciones de brechas, etc.

- Asesoramiento técnico a la Dirección de la AEPD, al Gabinete Jurídico en la elaboración de informes y al resto de unidades de la AEPD.

- Asesoramiento técnico a la SGPA en la promoción de códigos de conducta y en el análisis de consultas remitidas por el canal de menores.

- Asesoramiento técnico en la elaboración en guías y recomendaciones de otras unidades de la AEPD.

- Participación en los comités internos de la AEPD como: Comité de Coordinación, Criterios, Clasificación documental, Indicadores, Coordinación STIC, Coordinación Informática, Comité de Seguridad, Grupo Igualdad, Grupo para uniformizar las comunicaciones con intervinientes en los procedimientos electrónicos y CANOA.

2.3.5. Mantenimiento y desarrollo de herramientas

En el marco, también, del impulso a la protección de datos, en particular, en el aspecto del desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de estos; además del mantenimiento de las herramientas Facilita y Gestiona, publicadas en años anteriores, se ha realizado las siguientes herramientas:

- *ASESORA-BRECHA* para asesorar a los responsables en sus decisiones relativas a la notificación de brechas a la autoridad de control.

- Revisión y actualización a entorno web de la herramienta *EVALÚA-RIESGO* para permitir la identificación y evaluación del riesgo para los derechos y libertades de los interesados.

Además, se trabaja en la actualización y mantenimiento de las herramientas desarrolladas con anterioridad:

- *COMUNICA-BRECHA*

- Website Evidence Collector, una herramienta interna, para su uso por la SG de Inspección.

- *FACILITA*

- *FACILITA-EMPRENDE*

- *GESTIONA-RGPD*

La siguiente tabla muestra el número de accesos o veces que estas herramientas han sido utilizadas:

Herramientas	Núm. visitas
Facilita RGPD	56.575
Facilita EMPRENDE	3.525
Gestiona EIPD	34.049
Evalúa-Riesgo RGPD	101.897
Comunica-Brecha RGPD	4.830
Asesora-Brecha	3.811
TOTAL	**204.687**

En definitiva, el número de ejecuciones de las herramientas de privacidad desarrolladas por la DIT supera la cifra de 236.000 durante el año 2022.

2.3.6. Otras acciones de impulso a la responsabilidad proactiva

acciones realizadas por la UEET con el objeto de impulsar el cumplimiento del principio de responsabilidad activa del RGPD, en el marco del asesoramiento a emprendedores y desarrolladores tecnológicos con la finalidad de informar y asesorar en proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas han sido:

- Actualización de la sección *Innovación y Tecnología,* agrupando los contenidos tecnológicos por temáticas, en sus dos versiones en castellano e inglés.
- Mantenimiento de la sección *Lucha Contra la Violencia de Género y la Violencia Digital* con una actualización publicada el 25 de noviembre.
- Mantenimiento de la sección *Brechas de datos personales.*

Por otra parte, los miembros de la DIT han participado en la elaboración de numerosas cuñas de radio sobre temas tecnológicos, actividades de formación externa e interna, así como divulgación en temas de protección de datos.

Desde la DIT también se viene dando soporte al canal de Atención al Ciudadano con relación a las consultas de los responsables de índole técnica, en general consultas relacionadas con aspectos sobre evaluaciones de impacto, análisis de riesgos, medidas de seguridad, tecnologías, tratamientos biométricos, notificaciones de brechas, etc.

De forma general, la UEET participa en diversos grupos de trabajo con relación a proyectos e iniciativas técnicas y sobre tecnologías disruptivas que tienen impacto en protección de datos sobre temas de Big Data, Blockchain, Inteligencia Artificial, etc.

3. Al servicio de los ciudadanos. La protección de las personas en un mundo digital

La presencia de la tecnología en la vida diaria de las personas nos define como sociedad digital en la que, como en el mundo offline, tenemos que proteger a las personas de los riesgos y las consecuencias que pueden derivarse de su falta de capacitación y formación para utilizarla, o de su uso irresponsable, como adiciones o usos problemáticos, ciberacosos, extorsiones y violencia digital. Protección que compete a todos los poderes públicos mediante medidas dirigidas a evitar o disminuir los daños y perjuicios que pueda ocasionar su utilización de manera inapropiada.

3.1. Adaptación de la actividad consultiva de la AEPD al RGPD: la Instrucción 1/2021 de la AEPD

La AEPD, de conformidad con las funciones atribuidas por el RGPD, la LOPDPGDD y la Instrucción 1/2021 de la AEPD, ha dado respuesta a las consultas individuales de los ciudadanos, tanto escritas – formuladas a través de la sede electrónica - como telefónicas, informando sobre la normativa aplicable relativa a sus derechos, cómo ejercerlos y, en su caso, la posibilidad y el modo de formular reclamaciones.

Se ha continuado con la actualización y mejora constante de las preguntas frecuentes (FAQs por su acrónimo inglés) publicadas en la web de la AEPD, con la finalidad de acercar y proporcionar de manera más accesible, ágil y clara el acceso de los ciudadanos a la información más demandada. Estas medidas de mejora han tenido un impacto inmediato en los usuarios, a través de una actualizada página web de la AEPD que, manteniendo todo su contenido y rigor, es sin embargo ahora más sencilla y accesible.

Los temas más frecuentes sobre los que versan las consultas son las reclamaciones ante la AEPD, dudas sobre la aplicación del RGPD, morosidad, videovigilancia y comunidades de vecinos.

En esta línea de constante mejora de la información que se facilita, han dado comienzo los trabajos para ofrecer un nuevo canal de respuesta escrita inmediata automatizada (ChatBot), que comenzará a funcionar en 2023.

En cuanto a las materias de las consultas más frecuentes, a lo largo del año 2022, han sido las relacionadas con “reclamaciones”, seguidas por las consultas sobre la aplicación del “Reglamento General de Protección de Datos” y “derechos”.

Se mantiene la habitual fluctuación cíclica en el volumen de consultas en otras materias, como puede ser "videovigilancia", que aumenta significativamente al llegar el verano.

En este apartado cabe incluir la referencia a las quejas recibidas, respecto de las que se observa lo siguiente:

- Una utilización inadecuada del formulario de queja, que se usa para comunicar la oposición o desacuerdo ante determinados tratamientos de datos: publicidad spam, acoso publicitario, ficheros de morosos, cámaras de video vigilancia conflictivas…. Se trata de "quejas" frente a la actuación de otros responsables, o terceros. Estas quejas se canalizan y responden como consultas y computan a efectos estadísticos como consultas. En el período de referencia, de un total de 211 registros presentados con formulario de queja, 111 se han tramitado como consulta y sólo 100 han merecido la calificación de quejas, un 47 % del total.

- Continúa el aumento de las quejas que expresan un desacuerdo con los criterios de actuación de la Agencia ante las resoluciones recaídas sobre las reclamaciones que tramita la inspección de datos. Se utiliza la vía de las quejas en lugar, o como complemento a la vía del recurso procedente. No son propiamente quejas en el sentido previsto por el Real Decreto 951/2005, si bien se tramitan y responden como tales.

Se aprecia un ligero incremento del número de quejas propiamente dichas, en concreto, motivadas por la actuación del personal de la Agencia, por demora en las respuestas y por las incidencias técnicas que en determinados momentos han podido afectar al funcionamiento de los servicios electrónicos. El número pasa de 73 en el año 2021, a 100 en el 2022.

3.2. Nuevos espacios temáticos en la web

Con el objetivo de facilitar el acceso a la información, contenidos y recursos de la AEPD, además de las mejoras en las preguntas frecuentes (FAQs), se han aclarado y corregido contenidos, y de la puesta en marcha de un motor de búsqueda que permite la identificación de preguntas por palabras, se han creado dos nuevas áreas temáticas en la web que facilitan la búsqueda de la información y contenidos relativos al ámbito de la salud y de las Administraciones públicas.

La nueva Área de Salud incluye información y contenidos sobre las siguientes materias:

- *Tus derechos en relación con tus datos de salud*
- *Guías, informes del Gabinete Jurídico y consultas de Delegados de Protección de Datos sobre salud*
- *Protección de datos personales en la pandemia de COVID-19*
- *Investigación sanitaria y ensayos clínicos*
- *Principales reclamaciones en materia de salud*
- *Brechas de datos personales en el sector de la salud*

Desde su puesta en marcha, el 4 de mayo, el Área de Salud ha registrado 47.590 visitas.

El *Área de las Administraciones públicas* con la que se busca facilitar la tarea especialmente a los delegados de protección de datos del sector público, incluye la siguiente información y contenidos:

- Régimen general de los tratamientos realizados por las AAPP
- Guías, informes y documentos sobre los tratamientos de datos personales de las AAPP
- Instrucciones e informes
- Consultas más relevantes atendidas a través del Canal del DPD
- Brechas de datos personales
- Resoluciones relevantes sobre tratamientos de las AAPP
- Herramientas y Canal del DPD

Desde su puesta en marcha, el 3 de octubre, el Área de las Administraciones públicas ha registrado 9.354 visitas.

Los contenidos de ambas Áreas, como los de las demás, son objeto de constante actualización.

3.3. Educación y menores

La encuesta del INE sobre "Equipamiento y uso de TIC en los hogares" en 2022 recoge que el uso de Internet en los 3 meses anteriores por niños de 10 años fue del 90% y del 98,3% con 15 años.

El estudio de UNICEF sobre el "Impacto de la tecnología en la adolescencia", proporciona unos datos sobre el uso de las pantallas por los menores, que tuvo en la pandemia un elemento catalizador, que nos deben preocupar como sociedad. La edad media de acceso al primer móvil es de 10,96 años, y el 94,8% con acceso a Internet. El 31,5% usa Internet más de 5 horas al día, el 49,6% en fines de semana. 1 de cada 6 duermen con el móvil y 1 de cada 5 se conecta por la noche.

El 98,5% está en una red social y el 68,5% tiene más de un perfil. La conexión se produce para relacionarse con amigos y por diversión. Sin embargo, la falta de conocimiento sobre los peligros, así como de medidas preventivas y de supervisión para evitarlos pueden poner a muchos en serio riesgo de ciberacoso, grooming, sextorsión, adicciones al juego y apuestas o derivados de un uso problemático.

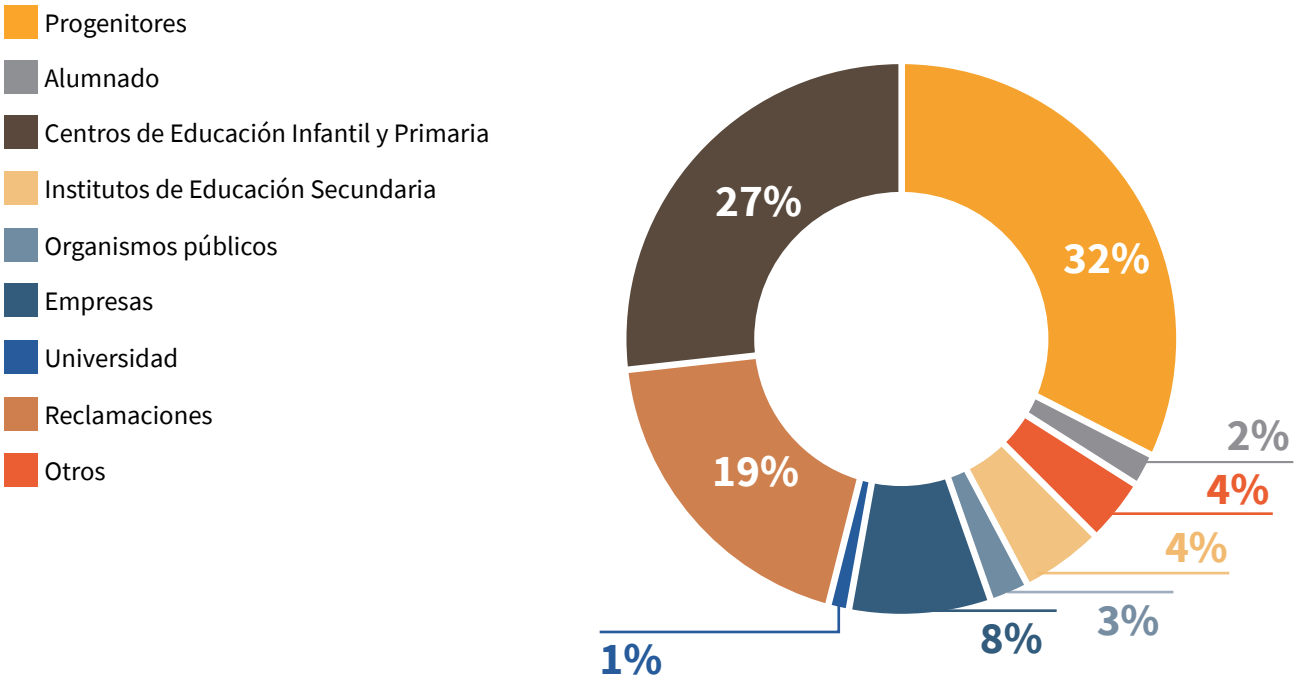
Mención específica merece la ideación o intentos de suicidio en los que están implicadas las tecnologías. Según el estudio de la Fundación ANAR "Conducta suicida y salud mental" la implicación de las tecnologías ha ido creciendo en los últimos años, con una tasa del 51% entre 2020 y 2021 que se traduce en un empleo abusivo e inadecuado. De los problemas asociados a conductas suicidas en niños menores de 10 años, el 47,8% incluía el ciberacoso.

El número de suicidios de menores de edad ha experimentado un crecimiento en los últimos años. Según datos del INE en 2019 se produjeron 7 suicidios de menores de 15 años, 14 en 2020 y 22 en 2021.

Estamos ante un problema de salud mental en el que el uso intensivo de la tecnología tiene mucho que ver, y que demuestra la necesidad de adoptar un Plan Nacional de Salud Mental Infantil y Juvenil para prevenir estas situaciones mediante pautas y criterios que, sobre la base de la evidencia científica, estén disponibles para familias, la comunidad educativa y el área de la salud.

Es necesario seguir insistiendo, por una parte, en medidas de prevención que conciencien a los menores para que hagan un uso razonable y saludable de Internet, en especial dirigidas al ámbito familiar y a la comunidad educativa, que incluya las responsabilidades penales, administrativas, civiles y educativas en las que se puede incurrir.

Por otra, en el refuerzo de la protección de los menores ante los riesgos de sufrir ciberacoso, grooming o sextorsión que, como muestras de violencia digital, tienen el Canal Prioritario de la Agencia una vía para poder evitar o disminuir los



daños, así como ante los riesgos de las adicciones o usos problemáticos de Internet.

La atención a los derechos de los menores de edad, en particular en el entorno educativo, se lleva a cabo a través de la Unidad de Educación y Menores y del espacio específico que se dispone en la web de la Agencia.

Las consultas recibidas y atendidas en esta Unidad, por los distintos canales que ofrece el *Canal joven* (dirección electrónica, teléfono específico y WhatsApp) y la *Sede electrónica* de la Agencia, durante 2022 han sido 2.368, lo que supone un incremento del 32% frente al 2021.

Destaca el gran número de llamadas recibidas (1.243) que supone el mayor incremento, desde que se inició la atención telefónica sobre los tratamientos de datos de menores, llegando al 120% frente a las recibidas en 2021.

Destacan las consultas que proceden de los progenitores (32%) sobre los tratamientos de datos de menores tanto en el ámbito educativo como en el plano personal. En este último aspecto se registran numerosas consultas sobre la publicación por familiares en redes sociales de imágenes de menores, en especial cuando los progenitores están separados y no existe relación cordial entre ellos por lo que no llegan a un acuerdo, Y aunque en principio esta difusión se podría considerar como de ámbito personal o doméstico (art. 2.2.c) RGPD) y por tanto excluido del ámbito de la normativa de protección de datos personales, la mayoría de familiares realizan la difusión en perfiles en abierto con un gran número de seguidores o bien en blogs propios. En estos casos se informa de que estas cuestiones se deben plantear ante el Juez competente.

En el plano educativo, se han incrementado las consultas de docentes y directores de centros educativos (8%), sobre tratamientos de datos en los centros escolares, argumentando el desconocimiento que tienen sobre la materia y la ayuda que necesitan. A este respecto se informa fundamentalmente utilizando la *Guía para centros educativos*, las distintas infografías publicadas y las *FAQs* de Menores y Educación. Además, se les deriva a la figura de la persona designada *Delegada de Protección de datos*.

También, se han recibido más consultas procedentes de empresas privadas (8%) que tratan datos personales de menores de edad, motivadas por la necesidad de conocer la normativa de protección de datos personales fundamentalmente en cuanto a tratamientos de videovigilancia y publicación de imágenes, con especial relevancia en el ámbito deportivo, en concreto de las competiciones organizadas por Federaciones Deportivas.

De Organismos Públicos se han recibido el (3%) de las consultas, procedentes especialmente de Policías Locales en relación con el tratamiento de datos de menores de edad, fundamentalmente en el desarrollo de competiciones deportivas en instalaciones de titularidad municipal o durante eventos o fiestas organizadas por las entidades locales.

Las consultas formuladas desde Universidades, tanto públicas como privadas (1%), proceden en su mayoría de profesores encargados de la dirección de los TFG, TGM y Tesis doctorales sobre los tratamientos de datos que implican.

Las consultas realizadas por alumnos universitarios y no universitarios suponen el 2% de las recibidas. La mayor preocupación que planteaban estaba referida a la comunicación de los centros educativos con los progenitores y la obligación de que éstos conocieran las calificaciones de sus hijos.

También, desde la Unidad de Educación y Menores se han tratado como consultas 34 de las 38 reclamaciones derivadas desde el Canal Prioritario que fueron recibidas en el acceso de 14 a 17 años, y que no reunían los elementos necesarios para su admisión en dicho canal.

Nuevos contenidos del espacio de Educación y Menores

De las consultas recibidas se detectó la necesidad de facilitar a las familias y a los profesionales, en especial los docentes, el acceso a la información de contacto de los Delegados de Protección de Datos de las Universidades, así como de los Servicios Públicos de Salud, que se sumaron a la relación ya existente de Administraciones y centros educativos:

- *DPD de Universidades* de las CC.AA.
- *DPD Servicios de Salud* de las CC.AA.

En la línea de proporcionar el fácil acceso y comprensión en este ámbito, se publicó una infografía sobre la *Actuación del coordinador/a de bienestar y protección del alumnado* en relación con la comunicación de contenido ilícito publicado y la solicitud de retirada de manera prioritaria, figura creada por la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI).

Así mismo, se incorporaron dos nuevas FAQ:

- *¿Están obligadas las Federaciones Deportivas a nombrar una persona que ejerza las funciones de delegado de protección de datos?*
- *En caso de separación, ¿tienen ambos progenitores derecho a recibir del centro educativo la misma información sobre el proceso formativo de sus hijos?*

En este año se ha producido la migración del portal de educación y menores al servidor de la AEPD y se ha modificado su línea de presentación para armonizarla al resto de espacios temáticos de la web.

Acciones dirigidas a la formación y sensibilización en el entorno educativo y de menores

La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD), incluyó en su artículo 83 el derecho a la educación digital, reiterado en el artículo 33 de la Ley Orgánica 8/2021, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI), cuyo objetivo es la plena inserción del

alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.

En la legislación educativa ha tenido su plasmación en la Ley Orgánica 3/2020, de reforma de la Ley Orgánica de Educación, que establece como uno de sus fines la capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales.

En desarrollo de dichos preceptos legales se han aprobado los Reales Decretos 157/2022 y 217/2022, que establecen la ordenación y las enseñanzas mínimas de la Educación Primaria y Secundaria Obligatoria, respectivamente.

En ambos Decretos se contempla, como perfil de salida del alumnado al término de la enseñanza en el marco de la competencia digital, el uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, para el trabajo y para la participación en la sociedad, así como la interacción con estas.

Y que se completa con la actualización del marco de referencia de la competencia digital docente (Resolución de 4 de mayo de 2022, de la Dirección General de Evaluación y Cooperación Territorial).

La Unidad de Educación y Menores colabora estrechamente con el INTEF y el INCIBE en la organización de actividades formativas en materia de educación digital dirigidas a la comunidad educativa:

NOOC Menores y seguridad en la Red (3ª edición)

16 y 25 de marzo

Esta experiencia formativa está dirigida a toda la comunidad educativa, pero especialmente a las familias. En esta edición se han matriculado 1.895 alumnos, fundamentalmente padres/madres y docentes. Incluyó una mesa redonda con la participación de expertos de las 3 instituciones que organizaban el curso. El video generado se publicó en el canal YouTube de INTEF y se puede consultar por cualquier persona *Mesa redonda: "Menores y seguridad en la red (3ª edición)" #MenorSeguroEnRed*

MOOC Educar en seguridad y privacidad digital (1ª edición)

Organizado por INCIBE, INTEF y AEPD

del 25 de octubre al 8 de diciembre

Dirigido a docentes de centros educativos no universitarios, se ha desarrollado del 25 de octubre al 8 de diciembre y ha contado con 3.240 alumnos.

El objetivo de esta experiencia de aprendizaje es ofrecer una visión general de las características de Internet y la tecnología (dispositivos, servicios y apps) que utilizan los profesores y los alumnos, de manera que el profesorado participante conozca y aplique pautas para ayudar a su alumnado a hacer un uso seguro y responsable de internet.

El MOOC incluyó un taller en el que 3 centros educativos seleccionados por su implicación en la materia explicaron sus experiencias, que fue difundido en streaming. *Disponible en YouTube*

Curso Tutorizado Protección de datos personales en centros educativos (2ª edición)

Organizado por INTEF y AEPD

del 11 de octubre al 14 de diciembre

Desarrollado del 11 de octubre al 14 de diciembre, ha contado 120 alumnos, dirigida a docentes de todas las etapas educativas no universitarias y de especial valor para inspectores de educación, miembros de equipos directivos, asesores de formación y asesores

técnico-docentes de las administraciones educativas y miembros de los departamentos de orientación y de equipos de orientación o de atención temprana.

3.4. Comunicación

Las acciones realizadas por Agencia en 2022 han estado acompañadas de sus respectivas iniciativas de comunicación con el objetivo de fomentar su difusión entre la ciudadanía, los responsables y encargados de tratamiento y los delegados de protección de datos. A continuación se recogen las relacionadas con el departamento de prensa y comunicación, así como la agenda institucional puesta en marcha por la AEPD para fomentar el conocimiento de las mismas.

3.4.1. Redes Sociales

Twitter y Youtube

La Agencia ha seguido en 2022 difundiendo materiales y consejos a través de la red social *Twitter*, incrementando en 2.000 los nuevos seguidores y con más de 1.000 tuits publicados este año. Superó así los 35.700 seguidores, siendo los tuits más destacados los siguientes: el inicio de oficio de actuaciones previas de investigación a TikTok, el lanzamiento de la guía básica de anonimización, consejos para compartir información en las redes sociales, la celebración del Día internacional de la protección de datos y consejos para proteger los datos personales cuando se contratan servicios de telefonía a distancia.

Asimismo, también se ha seguido trabajando en *el perfil que la Agencia mantiene abierto en YouTube*. La AEPD realiza contenidos multimedia con los que pretende facilitar la comprensión de algunos conceptos de protección de datos, así como difundir las iniciativas que lleva a cabo.

Este canal engloba cuatro tipologías de vídeos: la grabación de conferencias, charlas o webinarios organizados por la Agencia; vídeos con consejos o recomendaciones; videotutoriales para configurar las opciones de privacidad en navegadores, sistemas operativos, redes sociales y apps más populares, y las campañas de concienciación realizadas por la AEPD. En este sentido han cobrado especial relevancia los webinarios y conferencias de 'Mujer y ciencia' ya que, además de las visualizaciones que se producen en directo, los vídeos se publican en YouTube para que los usuarios puedan verlos en cualquier momento, difundiéndose asimismo a través del resto de redes sociales de la Agencia.

Los contenidos más vistos en YouTube en 2022 han sido el vídeo de la campaña 'Por todo lo que hay detrás' (Se suicidó porque todos vieron el vídeo en el que aparecía) y la configuración de las opciones de privacidad en TikTok, Facebook, Whatsapp y YouTube.

Los vídeos subidos a Youtube superan las 6.000 horas de visualización y se han visto más de 152.000 veces, un 10% más que en el mismo periodo del año anterior.

Lanzamiento del perfil en Instagram de la Agencia

La Agencia lanzó en septiembre de 2022 su perfil oficial en la red social *Instagram* **para potenciar tanto su presencia online en redes sociales como la difusión de los contenidos e iniciativas que realiza.** Instagram es una plataforma que alberga público de todo tipo y, especialmente, jóvenes, un grupo de destinatarios prioritario con los que la Agencia quiere conectar para promover la educación digital y que conozcan los derechos que les otorga la normativa de protección de datos y en qué puede ayudarles la Agencia.

La publicación con mayor alcance de 2022 está

relacionada con la campaña 'Más que un móvil', que se explicará con detalle posteriormente.

Activación del perfil en LinkedIn

La Agencia activó en mayo de 2022 su perfil en la red social *LinkedIn* para ampliar tanto su presencia online en redes sociales como la difusión de los contenidos e iniciativas que realiza. Al tratarse de una plataforma de networking, posibilita la conexión con una audiencia de carácter profesional, generando una cadena que hace que el contenido publicado sea más visible y llegue a un mayor número de destinatarios.

Aunque los temas son comunes con los que la Agencia aborda en otras redes sociales, las características propias de LinkedIn permiten explicar los asuntos que se difunden de forma más detallada, generando una reacción directa en los usuarios. Los temas más destacados que se abordan en el perfil de LinkedIn son los siguientes: Canal Prioritario, Informes jurídicos, Innovación y Tecnología, Eventos AEPD y días relevantes, Marco de Responsabilidad Social, Pacto Digital, Herramientas de la AEPD para pymes, startups y responsables de tratamiento de datos y vídeos de ámbito profesional sobre protección de datos.

Con más de un centenar de publicaciones realizadas desde su lanzamiento, el perfil de la Agencia terminó el año con casi 13.000 seguidores en esta red social, un crecimiento muy elevado que denota el interés de los profesionales en la protección de datos y los temas abordados en este perfil.

3.4.2. Otras acciones de difusión

Boletín informativo mensual AEPD

La Agencia lanzó en mayo de 2022 un nuevo boletín informativo mensual que tiene como destinatarias principales a las entidades adheridas al Pacto Digital. Ese boletín se publica, además, en *una nueva sección de la web*, de forma que todos aquellos que estén interesados puedan consultarlo. El objetivo del mismo es agrupar los lanzamientos y novedades de la Agencia orientadas fundamentalmente a responsables de tratamiento, aunque también recoge algunos temas centrados en el ciudadano, así como asuntos que, sin ser novedades, consideramos que pueden ser de utilidad.

El blog de la Agencia

El objetivo del *blog de la Agencia* es servir como altavoz para la difusión de diferentes iniciativas puestas en marcha, así como informes, guías, infografías o documentos, entre otras materias, aportando una visión cercana tanto del trabajo que se realiza en el organismo como de la protección de datos en un plano global.

Durante 2022 se han publicado 15 nuevos contenidos y entre los posts que han despertado un mayor interés se encuentran los relacionados con:

- *Metaverso y privacidad*

- *Anonimización y seudoaninimización*
- *Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos*
- *Difusión de vídeos con contenido violento en redes sociales*
- *Consejos para reforzar la privacidad en WhatsApp*
- *Blockchain (III): Smart contracts y datos personales*

Espacio 'Protegemos tu privacidad' de Radio 5

El espacio 'Protegemos tu privacidad' de la Agencia Española de Protección de Datos y Radio 5 ofrece a los ciudadanos recomendaciones para conocer sus derechos y saber cómo ejercerlos, así como consejos para facilitar el cumplimiento de la normativa a las organizaciones que tratan datos. Se estrena todos los miércoles y se realiza redifusión a lo largo de la semana, y todos los programas emitidos pueden escucharse en cualquier momento en la *página web de Radio 5.*

La emisión comenzó el 4 de julio de 2018 y desde entonces **se han emitido 194 piezas** temáticas en las que se ofrecen consejos y recomendaciones. **De ellas, 46 corresponden al año 2022.**

Relaciones con los medios

La difusión de la protección de datos por parte de los medios adquiere una gran importancia tanto por su contribución para concienciar a los ciudadanos en relación con sus derechos como difundiendo las obligaciones y la forma de cumplir los requerimientos establecidos en la normativa.

A lo largo de 2022, la Agencia **atendió más de 500 consultas** de medios de comunicación relacionadas con este derecho fundamental.

Esta labor de atención personalizada a los medios se vio complementada con el envío proactivo de notas de prensa a medios y a los departamentos de comunicación de las organizaciones adheridas al Pacto Digital. Asimismo, estas notas se publican en la página principal de la Agencia, habiendo recibido más de medio millón de visitas.

Las siete notas de prensa más consultadas en 2022 han sido las siguientes:

- *La AEPD publica una guía sobre protección de datos y relaciones laborales*
- *La AEPD publica una lista de verificación para ayudar a los responsables a realizar evaluaciones de impacto*
- *La AEPD publica una nueva guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto*
- *La AEPD lanza la versión online de Evalúa_Riesgo RGPD, que ayuda a valorar el nivel de riesgo de los tratamientos*
- *La AEPD y el Ministerio de Consumo lanzan una campaña con consejos para actuar ante una suplantación de identidad*
- *La AEPD publica una guía dirigida a los profesionales del sector sanitario*
- *La AEPD alcanza el 89% de cumplimiento en los compromisos adquiridos en su Plan de Responsabilidad Social 2019-2024*

Asimismo, en relación con notas de agenda informativa publicadas en la web, la Agencia publicó en 2022 más de 80 reuniones o actos públicos en los que participaron diferentes miembros de esta institución. Esta actividad de comunicación se vio complementada con la participación de la Agencia en las notas de prensa de las reuniones plenarias que periódicamente organiza el Comité Europeo de Protección de Datos (CEPD).

3.5. Agenda institucional

Durante 2022 la Agencia continuó con su misión de fomentar entre ciudadanos y organizaciones la cultura de la protección de datos, así como de contribuir al constante análisis de las implicaciones de la normativa de este derecho fundamental en la actividad de distintos sectores, mediante su participación virtual o presencial en numerosas reuniones, jornadas, foros, congresos, cursos, seminarios web, actos y presentaciones, como entidad organizadora o invitada. En paralelo, la Agencia siguió desarrollando iniciativas para visibilizar aún más su *Canal prioritario* de retirada de contenidos de carácter sexual o violento publicados en internet sin el consentimiento de las personas afectadas. La relación completa de la agenda institucional de la AEPD puede consultarse en la siguiente *sección web*.

Dentro del ámbito del sector público, la AEPD participó en diversos foros, congresos, cursos, comisiones, seminarios, reuniones y jornadas, como 'Juntos por una Internet mejor', organizada por la Consejería de Educación y Formación Profesional del Gobierno de Cantabria; las Jornadas sobre 'Inteligencia Artificial y género. Brechas, sesgos y nuevas formas de desigualdad', organizadas por la Universidad de Salamanca (USAL); el ciclo de sesiones 2022 del Foro de Sanidad y Derecho del Hospital Universitario La Paz; el IV Congreso de MSP – Mujer y Tecnología, organizado por la Asociación de Mujeres en el Sector Público; la II edición del Congreso de Seguridad Digital y Ciberinteligencia (C1b3rWall), organizado por la División de Formación y Perfeccionamiento de la Policía Nacional; la Comisión de Salud Digital del Consejo Interterritorial del Sistema Nacional de Salud; el Curso Superior en Protección de Datos organizado por la Escola Galega de Administración Pública; las Jornadas ASTICNET 2022, organizadas por la Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas (ASTIC); el 'Curso de Políticas Públicas en materia de Igualdad de trato y no Discriminación', organizado por el Ministerio de Justicia; el Seminario 'Retos, perspectivas y tendencias de la protección de datos', organizado por el Consejo General del Poder Judicial; el IV Seminario de Delitos de Odio, organizado por la Oficina Nacional de Lucha Contra los Delitos de Odio del Ministerio del Interior; las IV Jornadas de National Cyberleague de la Guardia Civil, o la VII Jornada de la UNED denominada 'Redes sociales: violencia digital'.

También intervino en cursos como 'Menores y seguridad en la red', un curso online nacido de la colaboración entre el Instituto Nacional de Tecnologías Educativas y Formación del Profesorado (INTEF), la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE), así como en la jornada 'La posición de la mujer en las organizaciones, bienestar organizacional y privacidad', en colaboración con la Asociación de Mujeres en el Sector Público, tras la cual se firmó un Protocolo General de Actuación entre ambas entidades para la colaboración en acciones de responsabilidad social en el ámbito de innovación, igualdad de género y protección de datos.

Asimismo, participó en encuentros digitales, como el destinado a hacer balance del primer año de vida de la Alianza País Pobreza Infantil Cero, en el que intervino el Alto Comisionado contra la Pobreza Infantil, Ernesto Gasco, y la directora de la Oficina, Carmen Gayo.

Además, la Agencia mantuvo reuniones en distintos ámbitos para impulsar el Canal prioritario, como la celebrada con la directora general de Derechos de la Infancia y la Adolescencia del Ministerio de Derechos Sociales y Agenda 2030, Lucía Losoviz Adani; las unidades de coordinación contra la violencia sobre la mujer y las unidades de violencia sobre la mujer; la consejera de Familia, Juventud y Política Social de la Comunidad de Madrid, Concepción Dancausa; el director general de Juventud de la Comunidad de Madrid, Nikolay Yordanov; el director general de Familia, Infancia y Dinamización Demográfica de la Xunta de Galicia, Jacobo Rey y la directora de la Agencia de Acceso a la Información Pública de Argentina (AAIP), Beatriz Anchorena;

En el ámbito ministerial, la AEPD celebró una reunión de carácter institucional con el Ministerio de la Presidencia, Relaciones con las Cortes e

Igualdad en el marco del Comité de Seguimiento del convenio suscrito entre ambas partes en 2019 para la valoración de las actuaciones en marcha y abordar nuevas propuestas.

En el marco de las relaciones de cooperación institucional entre autoridades, la AEPD mantuvo una reunión con representantes de la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

En el ámbito privado, la AEPD participó en la Jornada 'La aplicación de la normativa de protección de datos en las correduría de seguros', organizada por la Fundación ADECOSE; el World Bank Group Data Privacy Day 2022; el VIII Congreso de Regulación Publicitaria Digital, organizado por IAB Spain; el XIX Foro de Seguridad y Protección de Datos de la Salud, organizado por la Sociedad Española de Informática de la Salud con la colaboración de la Consejería de Sanidad de la Comunidad de Madrid; el XIV Foro de Privacidad del Data Privacy Institute; el Salón Internacional de la Seguridad (Sicur) 2022; la Jornada sobre protección de datos en instituciones de salud, organizada por la Alianza de la Sanidad Privada Española (ASPE) y Alaro Avant; el XXV Congreso Nacional de Informática de la Salud, organizado por la Sociedad Española de Informática de la Salud; el encuentro 'Tecnología en torno a la gestión del dato. Gestión de la privacidad en el Cloud', enmarcado en el Foro tecnológico de Europa Press; el VIII Congreso de Recursos Humanos, organizado por Foros Santander; la Jornada 'Seguridad y privacidad: Derechos y obligaciones de las Fuerzas y Cuerpos de Seguridad en materia de protección de datos', organizada por IPA Madrid (International Police Association) y ECIJA; el VIII Congreso Internacional de Privacidad, organizado por la Asociación Profesional Española de Privacidad; las I Jornadas Laboral-TECH, organizadas por el Consejo de la Abogacía Catalana y el seminario 'Estrategias para la protección de datos ante los desafíos del entorno digital', enmarcado en las Actividades de Verano 2022 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander.

Entre los actos en los que intervino la AEPD destacaron el encuentro 'Retos presentes y futuros del Delegado de Protección de Datos', organizado por ISMS Forum y la Asociación Profesional Española de Privacidad (APEP), en colaboración con la Agencia; el Seminario internacional 'Inteligencia artificial y protección de datos en investigación e innovación en salud: aspectos éticos, legales y sociales', organizado por el Observatorio de Bioética y Derecho, la Cátedra UNESCO de Bioética de la Universidad de Barcelona y la AEPD; el I Congreso Nacional del Deporte Autonómico, organizado por la Confederación de Uniones de Federaciones Autonómicas Deportivas Españolas (CUFADE); las III Jornadas 'La voz de los jóvenes ante el ciberacoso', organizadas por la Fundación Gestión y Participación Social y la Universidad Rey Juan Carlos I; el Seminario 'Investigación en salud: Desafíos del Espacio Europeo de Datos Sanitarios', organizado por la Cátedra Privacidad y Transformación Digital Microsoft-Universitat de Valencia; la 24ª edición de la Jornada Internacional de Seguridad de la Información, organizada por ISMS Forum; el V Congreso Educación Financiera de Edufinet; las III Jornadas 'El futuro de la economía de los datos', organizadas por Clúster Big Data Madrid; el X Congreso Internacional de Derecho Digital de la Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC) y el V Congreso de Privacidad del Club DPD, organizado por la Asociación Española para la Calidad.

La AEPD también mantuvo reuniones con representantes de fundaciones y asociaciones, como la Asociación Española de Fundraising (AEFr); la asociación Adigital; la asociación Adigital o la fundación COTEC. Por otra parte, la Agencia mantuvo una reunión con representantes de Microsoft, al objeto de que la corporación presentara la evolución de su propuesta de Perímetro Europeo de Datos (EU Data Boundary), así como su perspectiva sobre el marco transatlántico de privacidad de datos entre la Unión Europea y Estados Unidos.

Además, celebró una reunión de carácter institucional con la secretaria de Estado de Presupuestos y Gastos del Ministerio de Hacienda y Función

Pública, María José Gualda Romero, y con la subsecretaria de Justicia, Ana María Sánchez Hernández;

La AEPD también llevó a cabo diversos encuentros específicos enfocados a repasar la situación de distintos sectores en la aplicación de la normativa de protección de datos e intercambiar opiniones y buenas prácticas. Así, en el marco de su Instrucción 1/2021, la Agencia mantuvo encuentros con los Delegados de Protección de Datos de los centros docentes, públicos y privados, y otros actores de la comunidad educativa; de las Universidades; del sector sanitario público y otros actores privados; de la Administración General del Estado y de las Comunidades Autónomas, respectivamente, que se detallan en otro apartado de la memoria.

En este contexto, celebró una reunión con representantes de las vicesecretarías Generales Técnicas de los 22 Departamentos Ministeriales y los Delegados de Protección de Datos correspondientes al objeto de ofrecer pautas de actuación para la inclusión en los anteproyectos y proyectos de normas de carácter general de la evaluación del impacto en materia de protección de datos que acompañe a la Memoria de análisis de impacto normativo y permita la emisión del preceptivo informe por parte de la AEPD.

También participó en las I Jornadas Aragonesas de Protección de Datos, Transparencia y Ciberseguridad, organizadas por la Asociación Aragonesa de Delegados de Protección de Datos, y en las I Jornadas de la Asociación de Delegados y Delegadas de Protección de Datos de Parlamentos, organizadas por el Parlamento de Andalucía .Su detalle se describe en otros apartados de la memoria,

Por otra parte, la Agencia siguió dando cuenta de su actividad en distintas áreas, como la presentación de la *Memoria de Responsabilidad Social 2021*, que recoge sus compromisos con la sociedad, el buen gobierno, la integridad, la transparencia o la ética en línea con los Objetivos de Desarrollo Sostenible (ODS). También presentó nuevos recursos y materiales, como la *'Guía para profesionales del sector sanitario'*, un documento que da respuesta a las cuestiones más frecuentes que pueden surgir a los profesionales que intervienen en la prestación de servicios sanitarios con el objetivo de facilitarles el cumplimiento de la normativa de protección de datos y garantizar los derechos de los usuarios de estos servicios.

En el ámbito de menores, la Agencia celebró una reunión con representantes de los principales operadores de telecomunicaciones con la finalidad de colaborar en la difusión de campañas de concienciación dirigidas a las familias sobre el uso responsable por sus hijos/as de los dispositivos móviles, y presentó junto con UNICEF España la campaña *'Más que un móvil'*, dirigida a ofrecer a las familias las claves que deben tener en cuenta antes de entregar a sus hijos e hijas un teléfono móvil.

Por otra parte, la Agencia organizó un nuevo ciclo de debates digitales para analizar diversos aspectos relacionados con la ciencia y la tecnología, que se detallan en otro apartado de esta Memoria.

En el ámbito internacional, la Agencia continuó participando en las reuniones plenarias y los subgrupos del Comité Europeo de Protección de Datos (CEPD), así como en las reuniones digitales de febrero, junio y julio del Comité Ejecutivo de la Red Iberoamericana de Protección de Datos (RIPD) y mantuvo reuniones como la celebrada con los directores y directoras de las autoridades europeas de protección de datos, y la Comisionada del INAI, Norma Julieta del Río Venegas. La Agencia participó, asimismo, en la 15ª Conferencia internacional sobre Computación, Privacidad y Protección de Datos; en el coloquio 'Ciberseguridad: Las amenazas para Europa y el mundo en la nueva situación geopolítica', organizado por la Representación de la Comisión Europea en España, así como en la 44th Global Privacy Assembly.

En este contexto, la AEPD recibió la visita institucional del director-presidente de la Autoridad Nacional de Protección de Datos de Brasil, Waldemar Gonçalves Ortunho; de una delegación del Ministerio de Justicia de Cuba, y de la ministra de Telecomunicaciones y de la Sociedad de la Información de Ecuador, Vianna Maino.

En 2022, la AEPD siguió sumando entidades adheridas al *Pacto Digital para la Protección de las Personas*, una iniciativa de la Agencia que promueve un gran acuerdo por la convivencia en el ámbito digital con el doble objetivo de fomentar el compromiso con la privacidad en los modelos de negocio de empresas y organizaciones, y de concienciar a los ciudadanos de las consecuencias de difundir contenidos sensibles en internet. En este sentido, la Agencia se reunió con representantes de la ONCE para la firma por parte de esta de la adhesión al Pacto Digital. También se reunió con la vicepresidenta de la Asociación Europea para la Transición Digital, Ana Caballero, y la directora de comunicación del Club de Malasmadres, Carolina Martínez, para fomentar la difusión no sólo del Pacto Digital sino también del Canal Prioritario de la Agencia. Igualmente, la Agencia participó en las Jornadas Decide Madrid 2022 'Mirando hacia el futuro', organizadas por la Dirección General de Participación Ciudadana del Ayuntamiento de Madrid, donde la directora de la AEPD dedicó su intervención al Pacto Digital.

La Agencia también celebró reuniones dirigidas a la búsqueda de vías de colaboración con entidades como Unicef, concretamente en aspectos como campañas de sensibilización sobre el buen uso de Internet, la difusión de materiales, contenidos y herramientas para evitar situaciones dañinas en la red, la creación de nuevos contenidos o la formación de formadores o del personal de las organizaciones. En este sentido, también reunió con representantes de la Fundación del Instituto Internacional de Tecnología y Derecho Digital;

Por otra parte, la directora de la AEPD, Mar España, intervino ante la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo, para exponer la experiencia práctica atesorada por la Agencia respecto comenzó a aplicarse en mayo de 2018.

Finalmente, el Consejo Consultivo de la Agencia de Protección de Datos -órgano colegiado de asesoramiento a la dirección de la Agencia – mantuvo reuniones el 13 de julio y el 15 de diciembre de 2022 para exponer y analizar la actividad de la institución.

3.6. Infografías

La AEPD publicó en 2022 varias infografías como complemento a la información facilitada a través de sus canales. Todas ellas están disponibles en una *sección específica* de la página web de la Agencia y, aunque varias de ellas abordan temas que ya han sido tratados en formatos como guías u otros documentos más extensos, desde la Agencia se considera que este tipo de información puede ayudar tanto a los ciudadanos como a los responsables a abordar diferentes materias relacionadas con la protección de datos de una forma simplificada.

En 2022, se han publicado las siguientes infografías:

- *Responsabilidad de los menores (y de sus padres y madres) por los actos cometidos en internet*
- *Mapa de referencia para tratamientos que incluyen Inteligencia Artificial*
- *Cuándo y cómo se debe comunicar una brecha de datos a los afectados*
- *Actuación del coordinador/a de bienestar y rotección del alumnado*

3.7. Presentaciones

La AEPD continuó en 2022 con su compromiso de fomentar la cultura de protección de datos entre los ciudadanos y organizaciones a través de diferentes acciones de divulgación. La presencia física de los medios de comunicación a los actos se redujo en una parte del año por las medidas de control de la COVID-19, si bien se optó por una invitación para seguirlo en streaming cuando fue posible. El hecho de ofrecer seguimiento en directo de los actos organizados por la Agencia se ha mantenido incluso después de suprimirse las medidas COVID, al ampliar así el número de personas interesadas en seguir directamente las presentaciones.

Presentación de la campaña 'Más que un móvil' y 'La guía que no viene con el móvil'

10 de noviembre

La AEPD y UNICEF España lanzaron su campaña *'Más que un móvil'*, dirigida a ofrecer a las familias las claves que deben tener en cuenta antes de entregar a sus hijos e hijas un teléfono móvil. La campaña 'Más que un móvil' incluye el decálogo *'La guía que no viene con el móvil'*, que recoge pautas y recomendaciones para fomentar el diálogo y que las familias participen activamente en la educación de sus hijos e hijas, transmitiendo valores e información suficiente para garantizar tanto un uso responsable del teléfono móvil como los derechos de los niños y las niñas también en el entorno digital. La campaña cuenta con la colaboración de Movistar, Orange, Vodafone, Yoigo, Fundación Atresmedia, Mediaset España, RTVE, JC Decaux, Metro de Madrid y EMT Madrid, y su repercusión se detalla en otra parte de este documento.

Presentación Código de Conducta Farmaindustria

25 de febrero

La AEPD y Farmaindustria realizaron un acto presencial y retransmitido en streaming en el que se presentó el Código de conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia. Este nuevo código, promovido por Farmaindustria, se trató del primero sectorial aprobado desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD). En la presentación intervinieron Mar España, directora de la AEPD; Julián Prieto, subdirector general de promoción y autorizaciones de la AEPD; Humberto Arnés, presidente de Farmaindustria y Ana Bosch, directora del departamento jurídico de Farmaindustria.

Convenios de colaboración

En 2022 se celebraron los siguientes convenios de colaboración:

- Protocolo General de Actuación con la Unicef España (firmado el 16 de junio)
- Protocolo General de Actuación con la Asociación de Mujeres en el Sector Público (firmado el 4 de octubre)
- Protocolo General de Actuación con el IMSERSO (en tramitación)
- Protocolo General de Actuación con el Consejo de Colegios Oficiales de Psicólogos (en tramitación)
- Protocolo General de Actuación con el Patronato de Mayores y Pensionistas (en tramitación)

Apoyo a la investigación

del 14 de diciembre al 25 de febrero

El compromiso de la AEPD con las actividades de fomento y promoción alcanza también a la investigación que, además de los premios anuales que convoca, la favorece con la acogida de investigadores. Desde el 14 de diciembre de 2021 a 25 de febrero de 2022, la AEPD acogió a un profesor de derecho de la Universidad de Salamanca en una estancia de investigación para el desarrollo de su tesis doctoral "Cambio

de paradigma de la protección de datos de carácter personal y su interrelación con la sociedad digital.

3.7.1. Iniciativas de colaboración

Colaboración junto a INTEF para difundir el curso Menores y seguridad en la Red

La Agencia, el Instituto Nacional de Ciberseguridad (INCIBE) y el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF) lanzaron la 3ª edición del curso online gratuito 'Menores y seguridad en la Red', que tuvo lugar del 16 al 25 de marzo. La Agencia contribuyó a la difusión del mismo, tanto a través de su web de menores, sus redes sociales y su blog.

MOOC 'Educar en seguridad y privacidad digital'

La Agencia, en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, y el Ministerio de Educación y Formación Profesional, a través del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), realizaron un curso de formación gratuito en formato MOOC, dirigido a los docentes, durante diciembre de 2022. Al igual que con el mencionado anteriormente, la Agencia colaboró también con la difusión del mismo, tanto a través de su web de menores, sus redes sociales y su blog.

Colaboración con la Delegación de Gobierno contra la violencia de género

La Agencia ha colaborado con la Delegación de Gobierno contra la violencia de género, entre otros temas, con la adaptación del Decálogo para medios de comunicación y organizaciones incluido en el Pacto Digital para la Protección de las Personas. El objetivo de la Delegación es divulgarlo entre los medios incluyendo un código QR para su descarga directa. Asimismo, el canal prioritario de la Agencia se ha difundido en edición 2022 del festival Womad de Cáceres dentro del Punto Violeta, puesto en marcha por el Instituto de la Mujer de Extremadura (IMEX), el Ayuntamiento cacereño, la Diputación Provincial de Cáceres y la Subdelegación del Gobierno.

Difusión del Canal prioritario por parte de las universidades

El 3 de mayo de 2022 la Agencia mantuvo un encuentro con los delegados de protección de datos de las Universidades con la finalidad de repasar la situación del sector en la aplicación de la normativa e intercambiar opiniones y buenas prácticas. Uno de los puntos que se trató fue la difusión del Canal prioritario por parte de las Universidades, ya que la Agencia considera que es importante que el público universitario conozca la existencia de este Canal para denunciar la difusión en Internet de contenidos sexuales o violentos.

Con la **colaboración del Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)**, las universidades andaluzas han sido las más activas en la promoción de esta iniciativa. Para todas las universidades que lo han pedido, la Agencia ha adaptado su cartel 'Por ti y por todxs tus compañerxs', añadiendo su logotipo junto al de la AEPD y el Ministerio de Educación, y el del CTPDA en el caso de tratarse de una universidad de Andalucía.

Las universidades que han colaborado activamente son las siguientes: Almería, Granada, Jaén, Málaga, Sevilla, Pablo de Olavide. También se ha sumado a la campaña la Universidad Católica de Valencia, la UNIR y la Universidad de las Illes Balears, y se sigue trabajando para que se incorporen otras universidades.

Acerca de la difusión realizada junto con el CTPDA por las Universidades de Andalucía, se pueden extraer los siguientes datos relevantes:

- Las universidades de Jaén, Granada y Málaga han valorado el impacto de esta campaña en 45.557 estudiantes y casi 9.000 trabajadores y personal investigador.

- La Universidad de Almería realizó una tirada en imprenta del cartel en formato A3 y a color. En cada uno de los edificios de la UAL se colgaron dos carteles como mínimo, en zonas de máxima visibilidad y publicidad para el alumnado. También se tiene el cartel en la pantalla interactiva de información del Edificio Central de la Universidad.

Todas las universidades han difundido su iniciativa a través de sus redes sociales y los canales digitales internos de los que disponen para comunicarse con los alumnos, como la inclusión de carteles y vídeo en el Sistema de Comunicación Dinámico de la Universidad de Jaén, además de en los boletines internos que realizan las universidades.

3.7.2. Campañas de difusión

Campaña ‘Más que un móvil’ + La guía que no viene con el móvil con UNICEF España

La AEPD y UNICEF España lanzaron el 10 de noviembre su campaña *‘Más que un móvil’*, dirigida a ofrecer a las familias las claves que deben tener en cuenta antes de entregar a sus hijos e hijas un teléfono móvil. La campaña contó con la colaboración de Movistar, Orange, Vodafone, Yoigo, Fundación Atresmedia, Mediaset España, RTVE, JC Decaux, Metro de Madrid y EMT Madrid, que la han difundido a través de sus respectivos canales para que todas las familias tengan acceso a unos consejos básicos sobre cómo pueden preparar a sus hijos e hijas para el acceso a estas tecnologías

La campaña ‘Más que un móvil’ incluye el decálogo *‘La guía que no viene con el móvil’*, que recoge pautas y recomendaciones para fomentar el diálogo y que las familias participen activamente en la educación de sus hijos e hijas, transmitiendo valores e información suficiente para garantizar tanto un uso responsable del teléfono móvil como los derechos de los niños y las niñas también en el entorno digital.

La campaña se centra en la idea de que se le da un teléfono móvil a un niño o a una niña… “y ya”. Ese “y ya” puede ser el punto de partida de una buena experiencia o el comienzo de una serie de problemas a los que en ocasiones resulta difícil enfrentarse a posteriori (envío de fotos comprometidas, ciberacoso, contactos con personas adultas que se hacen pasar por menores, dejar de hacer actividades en la vida real para estar siempre conectado, etc.).

En cuanto a los colaboradores de la campaña, ha sido la primera vez en la que participan de forma conjunta Movistar, Orange, Vodafone y Yoigo, que la incluyeron en las pantallas digitales de sus puntos de venta, añadieron el código QR para descargar el decálogo de consejos ‘La guía que no viene con el móvil’ junto a los terminales que comercializan o la incorporaron a los materiales en sus programas de formación, entre otras acciones de difusión. Asimismo, Atresmedia, Mediaset y RTVE la emitieron en sus respectivos canales el spot de servicio público, una acción que también llevarán a cabo Movistar Plus+ y Vodafone TV. Por su parte, JC Decaux ha realizado difusión de la misma a través de su cartelería tanto de calle como de centros comerciales, y Metro de Madrid y EMT Madrid también han difundido la iniciativa en sus respectivos canales. Estos colaboradores se vieron incrementados tras el lanzamiento inicial de la campaña con la contribución de las redes sociales de META (Facebook e Instagram), que se sumaron a la difusión de la misma con una cesión de inversión publicitaria en tres momentos puntuales: tras las navidades (al considerarse un momento estratégico en la entrega de un móvil a los niños y niñas), el 28 de enero de 2023 (Día internacional de la protección de datos) y el 7 de febrero de 2023 (Día de Internet segura). Estos tres hitos de la campaña quedan fuera del marco temporal de esta Memoria.

A esta difusión realizada por los colaboradores hay que sumar la repercusión orgánica de la noticia de la campaña en los medios de comunicación y en las redes sociales tanto de la Agencia como de UNICEF España. Teniendo en cuenta todo ello, la repercusión acumulada de la campaña en 2022 ha sido de más de 290 millones de impactos. Además, como se ha comentado con anterioridad, la campaña sigue vigente fuera del marco temporal de esta Memoria como, por ejemplo, a través de la difusión realizada en cartelería de calle y centros comerciales por JC Decaux, lo que generará un incremento en los impactos realizados en 2023. Además, durante 2023 se está trabajando con otros organismos, entidades, instituciones y asociaciones para seguir promoviendo pautas y recomendaciones para que las familias participen activamente en la educación digital de sus hijos e hijas.

Campaña junto al Ministerio de Consumo con consejos para actuar ante una suplantación de identidad

La Agencia y el Ministerio de Consumo lanzaron el 28 de enero una campaña en redes sociales para difundir entre la ciudadanía *qué pasos deben seguir si sufren una suplantación de identidad en estos las redes sociales*. Esta campaña coincidió con la celebración del Día Internacional de la Protección de Datos, una jornada impulsada por la Comisión Europea, el Consejo de Europa y las autoridades de protección de datos de los Estados miembros de la UE con el objetivo de impulsar entre los ciudadanos el conocimiento de sus derechos en materia de protección de datos. La campaña, que se sigue difundiendo en redes sociales, detalla qué pasos se deben seguir para eliminar el perfil falso de la manera más rápida posible, para lo que es necesario contactar en primer lugar con la red social mediante los formularios habilitados a tal efecto. Además, indica qué hacer si alguien publica contenidos sexuales o violentos de terceros sin su consentimiento, como acudir al Canal prioritario, ya que por la especial gravedad de estas situaciones, no es necesario contactar primero con la web o la red social en la que están publicadas.

Colaboración con Clan TV (RTVE) en vídeos educativos para menores

Del 1 al 13 de febrero de 2022 Clan puso en marcha con la colaboración de la Agencia la campaña 'Juntos por una internet mejor' para fomentar entre los menores el uso seguro de internet. La campaña contó con piezas informativas con consejos saludables en el uso de internet, tanto sobre los contenidos que se ven como acerca los riesgos del abuso de la red, la huella digital, o protección contra el ciberacoso.

La campaña estuvo dirigida a los niños más pequeños, fundamentalmente de preescolar e infantil. Entre los mensajes, cuestiones como que sólo se comparten contenidos que se podrían ver en casa también; que la noche es para dormir y no para chatear; que para navegar con seguridad hay que hacerlo en compañía; o que entre amigos es más divertido charlar que chatear.

3.7.3. Premios

Premios concedidos por la AEPD

La Agencia entregó el 28 de enero de 2022 los 'Premios Protección de Datos 2021' en las categorías de Comunicación, Investigación 'Emilio Aced', Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD, Buenas prácticas educativas y Buenas prácticas para la protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género.

En la categoría de Comunicación, la AEPD entregó el premio a Atresmedia por sus campañas de difusión de diversas iniciativas comprometidas con la protección de datos. En concreto, el grupo de comunicación se ha hecho eco de las campañas de comunicación sobre el *Pacto Digital para la Protección de las Personas y el I Foro de Privacidad, Innovación y Sostenibilidad*; *'Un solo clic puede arruinarte la vida'*, *'Lo paras o lo pasas'*, así como otros contenidos de difusión específicos del *Canal prioritario* para solicitar la retirada de contenidos de carácter sexual o violento publicados en internet sin el consentimiento de las personas afectadas.

El jurado otorgó un accésit en esta misma categoría a Gabriel Cruz García por su reportaje 'Canal prioritario contra el bullying', emitido en informativos Cuatro Fin de semana, distribuido a través de la agencia ATLAS y difundido en las páginas web de la plataforma Mediaset, en el que se aborda cómo el Canal prioritario de la AEPD puede ayudar a luchar contra el acoso escolar.

En la categoría de 'Investigación en protección de datos personales Emilio Aced' el jurado concedió el premio a Narseo Vallina Rodríguez, Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On y Serge Egelman, por su trabajo '50 Ways to Leak Your Data: An exploration of Apps' Circumvention of the Android Permissions System', relacionado con la investigación en el marco del proyecto AppCensus que se presentó ante el Comité Europeo de Protección de Datos.
Asimismo, el jurado otorgó un accésit a María Martín Pardo de Vera, por su trabajo 'Innovación, privacidad e igualdad'. La autora, responsable de la Comisión de Tecnología de Women in a Legal World, realiza un análisis holístico en el que relaciona innovación, protección de datos e igualdad.

Respecto al Premio a la Proactividad y Buenas Prácticas en el cumplimiento del Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales (LOPDGDD), en la modalidad de empresas, asociaciones y fundaciones, el jurado concedió el premio a DataForGoodBCN, por su trabajo 'Transferencia de datos cifrados preservando la privacidad en federación de entidades sociales', que pretende promover, coordinar y atender a las diferentes asociaciones y entidades de iniciativa social dedicadas a la defensa de los derechos y la inclusión de las personas con síndrome de Down de Cataluña y de sus familias. En el trabajo ha colaborado la coordinadora Down Catalunya, así como la Universidad Pompeu Fabra.

Por otra parte, el jurado concedió un accésit a la Fundación CNSE para la supresión de las barreras de comunicación, por su trabajo 'Accesibilidad de las personas sordas al RGPD', que consiste en una página web accesible con información sobre los derechos que confiere el Reglamento General de Protección de Datos, con información y vídeos en lengua de signos y enlaces a los formularios para el ejercicio de derechos y presentación de reclamaciones, contribuyendo a la creación de una cultura de protección de datos entre las personas sordas.

Dentro del Premio a la Proactividad y Buenas Prácticas en el cumplimiento del RGPD y la LOPDGDD, en la modalidad de entidades del sector público se otorgó el premio al Colegio de Registradores de la Propiedad y Mercantiles de España (CORPME), por su trabajo 'Buenas prácticas para la centralización del cumplimiento del RGPD', una guía elaborada en colaboración con Unión Profesional para servir de ayuda a la implementación o mejora de un servicio centralizado de protección de datos que optimice y mejore los sistemas de cumplimiento y reduzca costes de implantación a los responsables de tratamiento, a la vez que

garantice los derechos de los ciudadanos en materia de protección de datos.

El jurado concedió en esta misma categoría un accésit a la Diputación Foral de Bizkaia, por su 'Plan de adecuación a la normativa de protección de datos del sector público foral del territorio histórico de Bizkaia', un modelo de organización y gestión que recoge los principios generales, medidas de seguridad, procedimientos, responsables de aplicación y actividades de control y que enfoca su trabajo a la adopción de una política de privacidad que aúne protección de datos y seguridad de la información.

En la categoría '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 de Educación Primaria, ESO, Bachillerato y Formación Profesional, al IES Canónigo Manchón (Crevillent, Alicante), por su trabajo 'Ciberconvivencia emocional', que pretende concienciar al alumnado de primer ciclo de ESO sobre los riesgos de los dispositivos móviles. En él participaron alumnos de bachillerato para elaborar materiales, charlas y juegos que potencian el conocimiento de la materia.

En la modalidad de compromiso de personas, instituciones, organismos, entidades, organizaciones y asociaciones, públicas y privadas, se otorgó el premio al Consejo General de Colegios Profesionales de Ingeniería Informática, la Unidad de Psicología del Consumidor de la Universidad de Santiago de Compostela y UNICEF España, por el 'Estudio del impacto de la tecnología en los adolescentes', que analiza los hábitos de uso de internet y las redes sociales, y en el que han participado 50.000 alumnos de 265 centros educativos de Secundaria de todas las Comunidades Autónomas, con el fin de generar medidas y mecanismos de protección, educación y promoción de los derechos de niñas, niños y adolescentes en el entorno digital.

Finalmente, en la categoría de 'Buenas prácticas en relación con iniciativas del ámbito público y privado dirigidas a una mayor protección en internet de la privacidad de las mujeres víctimas de violencia por razón de género', el jurado premió a la Dirección General de Justicia e Interior de La Rioja, por su 'Protocolo de actuación para la detección e intervención con víctimas de violencia de género digital'. El protocolo, que pretende poner a disposición de la ciudanía y los agentes información y materiales para identificar y tratar problemas relacionados con la violencia de género, se aplica tanto en el Centro Asesor de la Mujer como en la Oficina de Asistencia a las Víctimas del Delito.

Premios recibidos por la AEPD

En 2022 la Agencia Española de Protección de Datos fue galardonada con un nuevo premio que se suma a los 18 que ha recogido desde 2017. En el marco de las IV Jornadas National Cyberleague de la Guardia Civil, la AEPD recibió un galardón de reconocimiento por su compromiso como colaborador institucional de la liga.

El histórico de premios recibidos por la AEPD puede consultarse *en este enlace*.

3.8. Acceso a la información pública y transparencia

Por lo que se refiere a la transparencia activa, es decir, la información que la AEPD hace pública a través de su propia web o distintos portales públicos, hay que señalar que en el informe de cumplimiento elaborado por el Consejo de Transparencia y Buen Gobierno en febrero de 2022, se hizo constar que el Índice de Cumplimiento de la Información Obligatoria (ICIO) se sitúa en el 95,2%. Respecto de 2021 se produce un incremento de 17,5 puntos porcentuales atribuibles a la aplicación de una de las recomendaciones efectuadas en 2021.

El CTBG concluyó que valoraba muy positivamente la evolución del cumplimiento de las obligaciones de publicidad activa por parte de la AEPD. Se han aplicado todas las recomendaciones efectuadas como consecuencia de la evaluación realizada en 2021.

En cuanto a la transparencia reactiva, o solicitudes de acceso a la información pública, se constata la tendencia iniciada hace dos años de aumento en el número de solicitudes de acceso a información pública. La mayor parte de las peticiones se refieren a expedientes y resoluciones sancionadoras. También se han solicitado, y se ha facilitado, el acceso a informes de la AEPD, información sobre la actividad internacional de la AEPD, sobre sus gastos, y sobre actividades de colaboración con otros organismos de la AGE.

En 2022, ha aumentado el número de concesiones de acceso, tanto concesiones totales como parciales. Hay que señalar igualmente que el 100% de las resoluciones de acceso adoptadas por la AEPD se han producido dentro del plazo legalmente establecido para resolver. En este periodo, 6 resoluciones de la AEPD fueron recurridas ante el Consejo de Transparencia y Buen Gobierno (CTBG), de las que se han resuelto 4 y se han desestimado las 4. En estos casos, se ha confirmado por el CTBG el criterio adoptado en la resolución AEPD. En dos de ellas, la AEPD razonaba en sus resoluciones que la solicitud de acceso en cuestión era un recurso encubierto frente a una resolución de la AEPD y esta no es la vía legal para recurrir ese tipo de resoluciones. Criterio confirmado íntegramente por el CTBG.

Así mismo, el CTBG confirmó el criterio de la AEPD de que el acceso a la información pública no es sólo acceso a documentos, sino que, cuando esto sea lo procedente, puede ser también acceso a información sobre el estado de situación de un asunto y de cómo la AEPD ha procedido, en particular, el solicitante solicitaba una resolución expresa sobre una reclamación que había sido acumulada a otra en el mismo expediente durante la tramitación del procedimiento; la AEPD informó sobre el resultado de la tramitación llevada a cabo. El CTBG también ha confirmado el criterio de la AEPD de denegar el acceso cuando éste puede perjudicar investigaciones en curso o el proceso de toma de decisiones. (Cfr. Resoluciones del CTBG números de referencia: 81/2022; 195/2022; 449/2022; 452/2022).

La Unidad de Información y Transparencia (UIT) de la AEPD participa en el grupo de trabajo del Comité Europeo de Protección de Datos preparando el estudio europeo comparado sobre el acceso a documentos de expedientes sancionadores y actuaciones de investigación transfronteriza. Igualmente, la UIT de la AEPD participa en el grupo de trabajo que aglutina a todas las UITs de la Administración General del Estado (AGE) para coordinación de criterios, que es convocado y dirigido por la DG de Gobernanza.

En aplicación de su compromiso de actuación transparente, la AEPD publica en su web las resoluciones firmes denegatorias, o parcialmente denegatorias, para el conocimiento general de los razonamientos y motivación de su actuación *https://www.aepd.es/es/la-agencia/transparencia/resoluciones-de-transparencia*

4. Ayuda efectiva a las entidades

4.1. Sujetos obligados y delegados de protección de datos (DPD): funcionamiento del Canal del DPD y valoración de las consultas de los DPD

Los sujetos obligados, responsables y encargados del tratamiento, deben cumplir con el principio de responsabilidad proactiva que se complementa con la obligación, en unos casos o la posibilidad, en otros, de designar un DPD, a través del cual se pueden formular consultas a la AEPD.

En virtud del artículo 39.1.e) del RGPD y conforme a los requisitos que se exponen en la norma 4 de la Instrucción 1/2021, la AEPD puede ser consultada por los DPD, bajo ciertos requisitos coherentes con el principio de responsabilidad proactiva, y por las organizaciones y asociaciones representativas de responsables y encargados del tratamiento que presten servicio de asesoramiento en materia de protección de datos a sus asociados, especialmente cuando se trate de pequeñas y micro empresas, en las mismas condiciones que se establecen para los DPD.

Como viene ocurriendo desde la puesta en marcha del Canal del DPD, las consultas se responden con base en los criterios previamente establecidos por el Gabinete Jurídico de la Agencia.

Sobre las consultas recibidas en este año 2022, que ascienden a un total de 695, se pueden resaltar como más relevantes, las siguientes:

En el ámbito de las **Administraciones públicas** se han planteado diferentes cuestiones sobre el intercambio de datos a través de las plataformas de intermediación y comunicación de datos entre Administraciones públicas que han sido respondidas conforme a la interpretación recogida en el informe 175/2018 del Gabinete Jurídico de esta AEPD *https://www.aepd.es/es/documento/2018-0175.pdf*

La instalación de cámaras con fines de seguridad, control del tráfico y prevención de delitos, junto a las obligaciones derivadas de la aplicación de la normativa de protección de datos sigue siendo un tema muy recurrente en el ámbito de la Administración Local. Para resolver este tipo de dudas la AEPD dispone de un apartado en su web dedicado a la videovigilancia y de una guía específica de protección de Datos en la Administración Local, además de las preguntas frecuentes que sobre esta materia se han elaborado.

Las consultas relacionadas con el tratamiento de datos personales en el ámbito laboral más reiteradas han versado sobre el acceso a los datos incluidos en el registro de jornada, en la coordinación de actividades empresariales y el tratamiento de datos relacionados con la vigilancia de la salud de las personas trabajadoras y el acceso a sus datos por parte de los representantes sindicales. Para la respuesta a estas cuestiones se han considerado los criterios reflejados en la Guía sobre protección de datos y relaciones laborales.

La publicación de datos en supuestos de procedimientos de concurrencia competitiva, concesión de subvenciones, adjudicación de contratos del Estado y en ejercicio del derecho de oposición por parte, entre otras, de personas víctimas de violencia de género, también son aspectos que suscitan dudas a los DPD en las Administraciones públicas en general. Para resolver estas dudas, en la página web de la AEPD se ha publicado una sección dedicada a los tratamientos llevados a cabo por las Administraciones públicas que incluye todos aquellos recursos que se encuentran disponibles para que puedan ser utilizados por los responsables y, especialmente, por las personas que tienen asignada la función de delegado de protección datos y sus equipos, facilitando así el ejercicio de su labor.

También han sido muy numerosas las consultas planteadas tanto por Administraciones públicas como por entidades privadas sobre la implanta-

ción de sistemas de reconocimiento facial para distintas finalidades, como entrada a bibliotecas, control de la presencialidad laboral, realización de exámenes online, identificación de pacientes en el ámbito sanitario, o procesos de identificación en oficinas bancarias. Sobre estas cuestiones, y partiendo de la posible desproporcionalidad del tratamiento de este tipo de datos biométricos por su consideración de categoría especial, se está debatiendo en el Comité Europeo de Protección de Datos y en la actualidad se han publicado las *"Directrices 05/2022 sobre el uso de técnicas de reconocimiento facial en el ámbito de aplicación de la ley"* que se encuentran en trámite de audiencia pública.

El uso de aplicaciones, plataformas y tecnologías digitales y su adecuación al RGPD en el sector educativo también está siendo objeto de consulta por parte de los DPD en la educación primaria, secundaria y universitaria, que solicitan el análisis de las aplicaciones y la elaboración de un listado de aquéllas que se puedan utilizar para la función educativa con garantía de que observan la normativa sobre el derecho a la protección de datos personales. En estos temas se ha aclarado que no es función de la AEPD su valoración porque es una actuación que el RGPD asigna a los responsables y encargados, en cumplimiento del principio de accountability.

Las condiciones de acceso a la historia clínica y la normativa de aplicación respecto al ejercicio de este derecho ha sido una cuestión planteada por parte de Administraciones sanitarias. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 18, regula el derecho de acceso a la historia clínica del paciente, derecho que está conectado con el propio derecho de acceso del artículo 15 del RGPD siendo competencia de la AEPD la atención de reclamaciones sobre el ejercicio de derechos y, en particular, el de acceso a la historia clínica.

4.2. Inscripción de Delegados de Protección de Datos Delegados de Protección de Datos (DPD)

Los DPD son una figura clave en el sistema de cumplimiento del RGPD, como resulta evidente de las funciones, posición y características que le atribuye, en particular su independencia en el ejercicio de sus funciones. Relevancia que también refuerza la LOPDPGDD.

El RGPD exige que los DPD se designen atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, lo que incluye un sólido conocimiento de su regulación, así como de la actividad en la que se ejercen sus funciones.

La AEPD, dada su importancia para el cumplimiento del RGPD y su supervisión, se ha interesado por conocer el estado de su situación transcurridos 4 años desde su aplicación efectiva, y les ha preguntado por los aspectos relativos a su designación, cualificación y el ejercicio de sus funciones con la finalidad de respaldar y reforzar la figura de los DPD. Para ello ha comenzado por el sector público y por determinados ámbitos de actividad, como el educativo y el sanitario, y ha consistido en enviar unas encuestas a los DPD de la Administración General del Estado, Órganos Constitucionales, Comunidades Autónomas y Universidades que, al igual que el ámbito educativo escolar y sanitario, tienen en el tratamiento de datos un elemento esencial para cumplir con sus respectivas finalidades.

Las respuestas recibidas mostraron diferentes grados de adaptación a la norma y, en muchas ocasiones, tendencias comunes. Aunque los resultados finales han de esperar los resultados de las encuestas a realizar en 2023, de las hasta ahora realizadas se puede adelantar que, con carácter general, los DPD no están dedicados en exclusividad a su labor en protección de datos, compartiendo funciones que no les permiten desarrollar sus funciones como DPD con la dedicación necesaria. De igual forma, no siempre

disponen de equipo suficiente y abogan por una mayor formación, tanto propia, para mantenerse actualizados, como de los miembros de sus equipos y de las organizaciones a las que prestan servicio. Se constata que no siempre participan en la gestión de nuevas normas, procedimientos o sistemas de información que respondan a tratamientos sobre datos de carácter personal. En muchas ocasiones no se ha regulado la posición de su figura dentro de la organización y, en muchas otras, se desconoce la necesidad de su figura como contacto con la Autoridad de Control.

Así, en el ámbito educativo y sanitario los DPD designados por parte de las Administraciones responsables son internos, de la propia organización. En otros órdenes de actuación pública no siempre se cumple esa condición, ni en la AGE, ni en las CCAA ni en las Universidades.

La oportunidad de este tipo de actuación ha quedado confirmada por el Comité Europeo de Protección de Datos (CEPD), que ha seleccionado como acción de evaluación coordinada para el año 2023 la misma materia, por lo que estos apuntes preliminares ha de servir para las conclusiones que ha de elaborar el CEPD como punto final de la acción coordinada.

En apoyo de los DPD en el ejercicio independiente de sus funciones, la AEPD, recuperando las actuaciones previas a la pandemia, ha mantenido Encuentros con los DPD de diferentes Administraciones públicas y sectores de actividad, tras los cuales se trasladó a los responsables la obligación que les incumbe de prestarles apoyo y recursos necesarios para que puedan ejercer sus funciones.

Estos Encuentros, celebrados en el marco de la Instrucción 1/2021, que dispone que la AEPD organizará jornadas, sesiones, seminarios, reuniones, tanto presenciales como online, y webinarios por sectores concretos de actividad en el marco de planes bienales, han sido los siguientes:

Sector Educativo
23 de mayo

Celebrado el 23 de mayo, reunió a los DPD de las Administraciones educativas, cuya actividad es competencia de la AEPD, y del Ministerio de Derechos Sociales y Agenda 2023, junto con los DPD y personas responsables de esta materia de las Organizaciones y Asociaciones educativas privadas. La creación de la figura del coordinador de bienestar y protección en los centros educativos por la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI) fue objeto de tratamiento en relación con la violencia digital pues su obligatoriedad es para el curso académico 22/23, para lo que se apuntó la realización de una acción formativa para 2023.

Sector Universitario
30 de mayo

El 30 de mayo se celebró el Encuentro con los DPD las Universidades, Públicas y Privadas y con la CRUE. Durante el mismo los DPD trasladaron algunas de sus preocupaciones, especialmente en relación con el tratamiento de datos que gestionan los alumnos en los TFG, TGM y Tesis doctorales, a cuyo respecto la CRUE manifestó que trabaja en la elaboración de cláusulas modelo para su adecuación al tratamiento específico, sin que a finales de año se hayan recibido en la AEPD.

Sector Sanitario
22 de junio

El Encuentro con los DPD del sector sanitario público y otros agentes del sector privado se celebró el 22 de junio. Durante el mismo tuvo lugar la presentación del espacio temático de la web de la AEPD sobre Salud y se plantearon cuestiones en materia de investigación con datos de salud para las que se apuntó la celebración en 2023 de talleres para su análisis.

Administración General del Estado y Órganos Constitucionales
28 de septiembre

El 28 de septiembre tuvo lugar el Encuentro con los DPD de la AGE. de los Órganos Constitucionales y de relevancia constitucional. Se recogieron las preocupaciones señaladas por los DPD, en particular la necesidad de disponer de más tiempo para el desarrollo de sus funciones, dado que las comparten con otras, y de equipo que en organizaciones como las ministeriales se hace necesario. También se presentó el espacio temático de la web de la AEPD sobre las Administraciones Públicas como lugar común de las cuestiones más habituales en protección de datos dentro de las Administraciones Públicas y que recopila consultas, informes y resoluciones de referencia en este ámbito.

Comunidades Autónomas
7 de noviembre

Los DPD de las 14 Comunidades Autónomas cuyo control es competencia de la AEPD (asistió también la persona delegada de protección de datos del País Vasco), además de las Ciudades Autónomas de Ceuta y Melilla. Durante el encuentro los DPD informaron de su situación y trasladaron preocupaciones en la misma línea que los DPD de la AGE, y a los que igualmente se presentó el espacio temático de la Web de la AEPD sobre Administraciones Públicas.

Por lo que respecta al número total de entidades que, a 31 de diciembre de 2022, han comunicado la designación y los datos de contacto de su delegado de protección de datos, en cumplimiento de lo estipulado en el artículo 37.7 del RGPD y el artículo 34.4 de la LOPDGDD, han sido 100.350, cuyos servicios se prestan por 12.181 DPD, de los que 2.516 son personas jurídicas y 9.600 personas físicas, que atienden a 73.560 y 26.790 responsables, respectivamente. Este dato supone un incremento en un 21% durante el año 2022, aunque representa un crecimiento menor, en un 4%, al incremento incorporado durante el año 2021.

Sin embargo, durante el año 2022 se recibieron un total de 20.562 comunicaciones, un incremento de un 7,4% sobre el total de comunicaciones recibidas en 2021. El número de comunicaciones de alta supone un 65% del total recibidas, las comunicaciones de baja representan un 25% y las comunicaciones de modificación son el 10% de todas las recibidas. Estos datos muestran el interés por los responsables en mantener actualizados los datos de contacto de su DPD.

Las Administraciones locales que han comunicado los datos de contacto de su DPD se ha incrementado en un 13,5% durante el 2022, llegando a un total de 4.537 responsables que han comunicado los datos de contacto de su DPD. La Administración Local sigue mostrando mayor crecimiento en sus comunicaciones entre todas las entidades con potestades públicas.

No obstante, se sigue constatando que todavía falta por designar, en su caso, y por comunicar a la AEPD los DPD por parte de entidades públicas, en particular de la Entidades Locales.

La Agencia procedió a trasladar esa carencia a los Ayuntamientos de más de 20.000 habitantes que no habían comunicado el DPD (un total de 60), con excepción de los de las Comunidades Autónomas de Cataluña, País Vasco y Andalucía; a las Diputaciones Provinciales (sólo 1) y las Universidades (en número de 6) que se encontraban en la misma situación.

4.3. Certificación de DPD conforme al Esquema AEPD – DPD

La cualificación de los DPD resulta fundamental para poder llevar a cabo sus funciones y desempeñar el papel que el RGPD y la LOPDPGDD les atribuyen como garantía del derecho fundamental a la protección de datos.

La AEPD con la finalidad de contribuir a la formación de los DPD y facilitar a responsables y encargados del tratamiento la designación de DPD cualificados elaboró un Esquema de Certificación en línea con lo que dispone el artículo 35 de la LOPDPGDD en julio de 2007.

En 2022 las principales magnitudes del Esquema tienen que ver con el número de DPD certificados, que han sido 138, el 48% de los 287 candidatos a obtenerlo en un total de 61 pruebas, a las que se ha incorporado una modalidad para personas con dislexia. Con ellos, el número total de DPD certificados con arreglo al Esquema de la AEPD a 31 de diciembre asciende a 927, dato que contrasta con el número de DPD que han sido comunicados a la AEPD.

Se mantiene en 8 el número de entidades certificadoras acreditadas por ENAC, al no haber avanzado el proceso para obtenerlas de dos entidades candidatas a ello.

En cuanto a las entidades de formación, la AEPD ha reconocido a la Universidad de León por su máster en "Derecho de la Ciberseguridad y Entorno Digital, Protección de Datos, Audiovisual y Sociedad de la Información", que se suma a la Universidad Carlos III. En preparación se encuentra el máster de otra Universidad que no ha concluido el proceso.

Durante este año comenzó la aplicación práctica de la Nota Técnica adoptada por la AEPD a finales de diciembre de 2021 con la que dar respuesta a las dudas que habían surgido con la aplicación del proceso de renovación de las certificaciones.

4.4. Códigos de Conducta

En este ámbito, la Agencia ha impulsado la elaboración de códigos de conducta que incluyan procedimientos de resolución extrajudicial de controversias en materia de protección de datos, procedimientos de mediación como instrumentos que facilitan una ágil y satisfactoria resolución de los conflictos, y que facilitan la correcta aplicación del RGPD, que los recoge como uno de los contenidos que se puede incluir en los códigos de conducta en su artículo 40.2.k).

Los procedimientos de resolución amistosa de reclamaciones son mecanismos útiles que ofrecen resultados positivos a las partes involucradas, como lo demuestran los resultados de la aplicación práctica del traslado a los DPD de las reclamaciones que se presentan ante la AEPD.

Los códigos de conducta aprobados por la AEPD en 2022 incluyen un procedimiento para la resolución de controversias en materia de protección de datos, que se añade al obligado procedimiento que los organismos de control y supervisión han de disponer para el incumplimiento de los propios códigos de conducta.

En cuanto a la actividad desarrollada durante 2022, y en la línea de años anteriores, se han mantenido numerosas reuniones y contactos con los promotores de códigos de conducta cuyos proyectos se encuentran en tramitación con la finalidad de ajustar su contenido a las exigencias del RGPD, las Directrices 1/2019 del CEPD y los criterios de acreditación de los organismos de supervisión adoptados por la Agencia, lo que implica el estudio y valoración de los proyectos presentados y de sus sucesivas versiones y, en su caso, efectuar las recomendaciones y sugerencias de mejora.

Las actuaciones realizadas han sido las siguientes:

Códigos de Conducta Nacionales

a) Códigos de conducta aprobados:

- El 10 de febrero de 2022 se aprobó el "CÓDIGO DE CONDUCTA REGULADOR DEL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO DE LOS ENSAYOS CLÍNICOS Y OTRAS INVESTIGACIONES CLÍNICAS Y DE LA FARMACOVIGILANCIA", cuyo promotor es la Asociación Nacional Empresarial de la Industria Farmacéutica (FARMAINDUSTRIA).

El ámbito objetivo de aplicación del código lo constituyen las actividades de tratamiento de datos personales en el marco de las investigaciones clínicas, en particular los ensayos clínicos, sobre la base del cumplimiento de una obligación legal en el tratamiento de los datos, así como las vinculadas al cumplimiento de las obligaciones impuestas por la normativa vigente en materia de farmacovigilancia para la detección y prevención de efectos adversos de los medicamentos ya comercializados. Asimismo, el código establece un procedimiento de mediación, voluntario y gratuito, que permite dar una respuesta ágil a las posibles reclamaciones que planteasen los interesados frente a las entidades adheridas.

- El 29 de junio de 2022 fue aprobado el "CÓDIGO DE CONDUCTA REGULADOR DEL TRATAMIENTO DE DATOS PERSONALES EN LOS SISTEMAS COMUNES DEL SECTOR ASEGURADOR", cuyo promotor es la unión Española de Entidades Aseguradoras (UNESPA).

El ámbito objetivo de aplicación del código lo constituyen las actividades de tratamiento de datos personales que se centran en el cumplimiento de las obligaciones que la legislación específica impone a las entidades aseguradoras adheridas como son las de adoptar medidas efectivas para prevenir, impedir, identificar, detectar, informar y remediar conductas fraudulentas relativas a seguros, para lo que se prevé la adopción de Sistemas de Información SIHSA, SIAPTRI y SIPFSRD (ficheros comunes) sin que sea necesario el consentimiento de los afectados. El código define la finalidad de los tratamientos de datos de cada uno de los Sistemas de Información: la realización de una valoración técnica y objetiva del riesgo, así como la correcta aplicación de las tarifas de prima en el Sistema SIHSA; y la prevención del fraude en los Sistemas SIAPTRI y SIPFSRD

- El 28 de noviembre de 2022 se aprobó la modificación del "CÓDIGO DE TRATAMIENTO DE DATOS EN LA ACTIVIDAD PUBLICITARIA" aprobado el 9 de octubre de 2020, promotor AUTOCONTROL.

Autocontrol ha actualizado el procedimiento de mediación en las controversias en materia sobre protección de datos en la actividad publicitaria, manteniendo las garantías de su contenido nuclear, con la finalidad de facilitar la adhesión de compañías que realicen actividades publicitarias y marketing.

b) Códigos de Conducta presentados para su aprobación y en tramitación

Continúa el laborioso proceso de adaptación de los antiguos códigos tipo aprobados (Disposición transitoria segunda LOPDPGDD) y de acompañamiento a los nuevos proyectos de códigos de conducta (Sección V del Capítulo IV del RGPD), por lo que una vez estudiada la documentación aportada y

elaborados los correspondientes informes, se han mantenido reuniones con los respectivos promotores que se relacionan a continuación:

- Unió Catalana d'Hospitales
- Associació Catalana de Recursos Asistencials (ACRA)
- Colegio Oficial de Farmacéuticos de Sevilla
- Asociación Nacional de Entidades de Gestión de Cobro (ANGECO)
- Confianza Online
- Asociación Española de Micropréstamos (AEMIP)
- Universidad Nacional de Educación a Distancia
- Universidad de Castilla La Mancha
- Asociación Nacional Para la Investigación de Marketing, Económica y Social
- (Antes ANEIMO y AEDEMO)
- Consejo Andaluz de Colegios de Administradores de Fincas

c) Iniciativas de códigos de conducta comunicadas

- Código de conducta de Firmas de Servicios Multidisciplinares (PwC, Deloitte, EY y KPMG)
- Código de conducta para empresas encargadas de tratamiento que realizan actividades de instalación y mantenimiento de equipos y sistemas de telecomunicación que conllevan tratamiento electrónico de datos personales (FECOTEL).

Códigos de Conducta Transnacionales

- La AEPD actúa como autoridad co-revisora en el proyecto de CÓDIGO DE CONDUCTA DE LA UE SOBRE INVESTIGACIÓN CIENTÍFICA, promovido por la Federación Europea de Industrias Farmacéuticas (EFPIA, por sus siglas en inglés).

4.5. Promoción del derecho fundamental a la protección de datos.

La AEPD, dentro del marco de promoción, realiza actuaciones de sensibilización dirigidas, por una parte, a responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD y la LOPDPGDD y, por otra, al público que incluye la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos, que se desarrollan a través de cursos, jornadas y participación en eventos que tienen por objeto las finalidades descritas.

Durante el primer semestre del año 2022 se registró una gran demanda de cursos sobre protección de datos por parte de organismos públicos, que llevó a que algunos se tuvieran que programar para el último trimestre del año e, incluso posponer, dados los limitados recursos disponibles y la carga de trabajo que peda sobre la AEPD.

La AEPD ofrece dos modalidades de cursos:

- Curso de 20 horas, impartido de forma presencial antes de la pandemia de la COVID y configurado en 8 videoconferencias en formato online.
- Curso de 6 módulos en formato Moodle. A principios de 2022 se actualizó todo el temario y se elaboraron nuevos casos prácticos y preguntas tipo test. Asimismo, se incorporó la realización de una videoconferencia en directo, en cada uno de los módulos, para una mayor interacción entre alumnos y profesor.

Además, se imparten cursos más específicos, adaptados a las características de las actividades de tratamiento de datos de los organismos y entidades, sujetos a la disponibilidad de la AEPD.

La formación impartida durante 2022, la gran mayoría online, se ha dirigido a:

- La Administración General del Estado: Ministerios de Educación y Formación Profesional; Interior; Sanidad; Defensa; Transporte, Movilidad y Agenda Urbana; Inclusión, Seguridad Social y Migraciones, en particular a la Tesorería General de la Seguridad Social; Universidades, Justicia, Trabajo y Economía Social; la Agencia Española del Medicamento y Productos Sanitario; la Agencia Española de Cooperación Internacional para el Desarrollo.
- Administraciones Autonómicas y Locales (Principado de Asturias y Ayuntamiento de Zamora)
- En este marco hay que destacar los cursos dirigidos a los empleados públicos que organiza el INAP sobre la "Aplicación del Reglamento General de Protección de Datos en las Administraciones Públicas", y que se imparten por representantes de la AEPD, que han contado con 600 alumnos.
- Formación que también se ha desarrollado en el ámbito interno impulsada por el delegado de protección de datos de la AEPD y por su Secretaría General en especial dirigida a los efectivos que se incorporan a la AEPD.

Se ha participado en esta labor de promoción y sensibilización en los siguientes cursos, y/o eventos:

- II Curso de Derechos Humanos, dirigido al personal de la Escala de Subinspección y Básica de la Policía Nacional.
- Máster de la Universidad Complutense de Madrid sobre Transparencia y Buen Gobierno.
- Curso selectivo de la 7ª promoción de facultativos del Instituto Nacional de Toxicología y Ciencias Forenses, organizado por el Centro de Estudios Jurídicos del Ministerio de Justicia.
- Instituto Regional de Seguridad y Salud en el Trabajo de la Consejería de Economía, Hacienda y Empleo de la Comunidad Autónoma de Madrid
- V Congreso Educación Financiera – Edufinet.
- 24 edición de la Jornada Internacional de Seguridad de la Información organizada por ISMS Forum.
- Participación en los Encuentros de la DPO Community de ISMS Forum.

Un aspecto importante de las actividades de promoción son las dirigidas a la difusión de las medidas adoptadas por la AEPD para la protección de colectivos vulnerables frente a situaciones de violencia digital, en particular del Canal Prioritario. En 2022 se ha intervenido en las siguientes Jornadas organizadas por:

- Consejería de Educación y Formación Profesional del Gobierno de Cantabria: dentro de la jornada.
- Universidad de Salamanca.
- Ministerio de Justicia: Curso de Políticas Públicas en materia de Igualdad de trato y no Discriminación.
- Consejo General del Poder Judicial.
- Fundación Gestión y Participación Social y la Universidad Rey Juan Carlos I.
- Oficina Nacional de Lucha Contra los Delitos de Odio del Ministerio del Interior.
- La Oficina de Igualdad de la UNED.

El Canal Prioritario su finalidad y funcionamiento también se ha difundido en el marco universitario a través de sus delegados de protección de datos, que contó para las Universidades públicas andaluzas con la colaboración del Consejo de Transparencia y Buen Gobierno de Andalucía.

Así mismo, la promoción y sensibilización de la protección de datos en el marco de la elaboración de disposiciones de carácter general originó la convocatoria, el 11 de noviembre de las Secretarías General Técnicas de los 22 Departamentos Ministeriales que componen el Gobierno de España, junto con sus respectivos DPD.

El objeto del Encuentro fue proporcionar orientaciones sobre las actuaciones a llevar a cabo en la preparación de anteproyectos y proyectos de normas de carácter general que ayuden a aplicar correctamente el principio de privacidad desde el diseño, y determinar la información que deben contener las memorias de análisis de impacto normativo (MAIN), análisis de riesgos, evaluaciones de impacto, de manera que permita a la AEPD emitir los informes preceptivos sobre la base de tratamientos de datos debidamente identificados y ofrecer un asesoramiento de utilidad.

Se expusieron como modelos de buenas prácticas los contenidos de la Ley Orgánica 20/2022, de 19 de octubre de Memoria Democrática y de la Ley 11/2021, de 28 de diciembre, de Lucha contra el Dopaje en el Deporte, cuyas disposiciones adicionales 10ª y 4ª, respectivamente, incluyen la regulación de los tratamientos de datos que implica la aplicación de sendas normas.

4.6. Transferencias internacionales

En materia de transferencias internacionales de datos, el año ha venido caracterizado por las negociaciones entre la Comisión Europea y la Administración de los Estados Unidos para alcanzar un marco de garantías que permita a aquélla adoptar una Decisión de adecuación para los Estados Unidos. Como consecuencia de las negociaciones la Comisión ha elaborado un proyecto de Decisión que se encuentra en tramitación con arreglo al procedimiento de decisiones de ejecución.

En el ámbito nacional, la actividad fundamental se ha desarrollado en relación con las normas corporativas vinculantes (BCR, por sus siglas en inglés). Así, durante 2022, una vez que el Comité Europeo de Protección de Datos emitió su opinión favorable, la AEPD ha aprobado las BCR del grupo multinacional Antolín que se suman a las BCR aprobadas en ejercicios anteriores lo que supone un total de 7 políticas de BCR ya adoptadas.

También durante 2022 se ha continuado con la revisión y tramitación, dentro del procedimiento coordinado establecido en el RGPD, de un total de 6 BCR que se encuentran en distinto grado de avance para llegar a obtener su aprobación.

Además, la AEPD ha participado como autoridad co-revisora en la tramitación de 7 proyectos de BCR lideradas por autoridades de protección de datos de otros Estados miembro en el marco también del procedimiento coordinado.

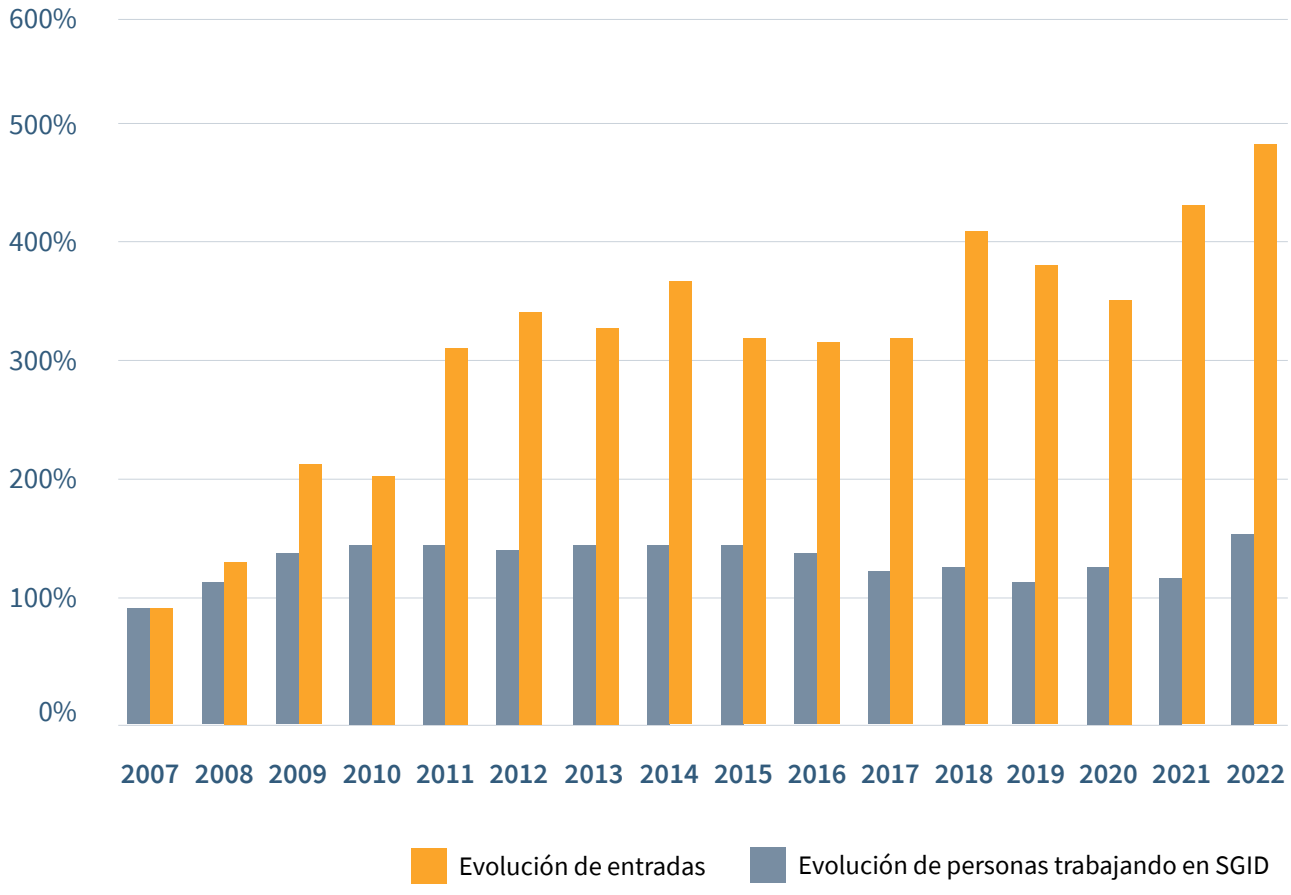
5. La potestad de supervisión

5.1. Resultados

La mayor presencia y alcance de los tratamientos de datos personales en la sociedad actual y la consiguiente preocupación de los ciudadanos por el tratamiento de sus datos vuelve a encontrar reflejo en el registro de reclamaciones ante la Agencia, que alcanza un año más un volumen sin precedentes. En 2022 se registraron 15.128 reclamaciones, un 9% más que el año inmediatamente anterior, y un 47% más que dos años antes.

La tasa de resolución de reclamaciones -que compara el número de reclamaciones recibidas con el número de reclamaciones resueltas en el mismo año- se ha logrado mantener en cifras cercanas al 100% (99% en 2022). La rápida evolución de los riesgos sobre la protección de los datos personales en la última década y media, derivado de la potencia y la ubicuidad de las nuevas tecnologías y de la globalización que supera los límites nacionales tradicionales, reclama un redimensionamiento de la Agencia que solo ha dado comienzo con la incorporación de catorce personas durante este último año, después de haber permanecido invariable durante los quince años anteriores.

Evolución compatariva del nº de entradas y del personal de la SGID, 2007- 2022



También se ha observado durante este último año una mayor extensión del ámbito de las reclamaciones e infracciones investigadas, con una menor presencia de casos individuales, y una mayor presencia de casos que afectan a una generalidad de afectados, por deficiencias de los procedimientos de tratamiento de datos personales. Este mayor alcance se refleja también en la amplitud de las actuaciones que la SGID desarrolla en respuesta a estos casos, que ya no precisan la investigación y corrección de un caso particular, sino el análisis y adecuación de los procedimientos del responsable a lo que exige la normativa.

El RGPD establece entre las funciones de la Agencia la de tratar las reclamaciones presentadas e investigarlas en la medida oportuna, informando al reclamante sobre el curso y el resultado. Esto se realiza en la SGID a través de las actuaciones y procedimientos que se regulan en el Título VIII de la LOPDGDD y, supletoriamente, en la regulación del procedimiento administrativo común que establece la LPACAP. La tramitación de las reclamaciones se inicia con una evaluación de la admisibilidad que incluye una primera fase de análisis previo de admisibilidad, para posteriormente desarrollar la fase de traslado de la reclamación al responsable o encargado y decidir sobre la admisión a trámite. Una vez admitida a trámite, si se estima necesario para determinar las circunstancias de la infracción y completar la identificación del responsable, se realizan las actuaciones previas de investigación, para finalmente, plantearse la procedencia de iniciar el procedimiento sancionador. En el caso de que la reclamación esté relacionada con los derechos establecidos en los artículos del 15 al 22 del RGPD, con la admisión a trámite de la reclamación se inicia un procedimiento de ejercicio de derechos. Cabe destacar que en 2022 se ha producido una revisión de los criterios que aconsejan la apertura de actuaciones de investigación previa al inicio de procedimiento, reduciéndose así el número de investigaciones un 22%, lo que al mismo tiempo ha permitido dedicar a los inspectores en mayor profundidad a las investigaciones efectivamente realizadas, una demanda inaplazable por la mayor complejidad de los casos, mejorando la eficacia de la investigación y reduciendo un 34% el número de investigaciones que concluyen en archivo de actuaciones.

A través de las actuaciones y procedimientos indicados se tramitan también otro tipo de entradas, distintas de las propias reclamaciones presentadas ante la Agencia, y que no existían con anterioridad a la aplicación del RGPD: casos procedentes de otras autoridades de control del Espacio Económico Europeo (EEE) y notificaciones de brechas de datos personales en las que procede su investigación por la SGID. También nace en años recientes el canal prioritario para la retirada de contenidos sensibles, como pueden ser fotografías, vídeos o audios de contenido sexual o violento que estén publicados en Internet. Este canal también incluye un acceso específico para los menores de 14 a 18 años. Todo ello, junto a las actuaciones realizadas por propia iniciativa, suman en 2022 cerca de 900 entradas adicionales a las reclamaciones que también originan las actuaciones descritas.

Además de las competencias que tiene la Agencia derivadas del RGPD y de la LOPDGDD, la Ley 11/2022 General de Telecomunicaciones (en adelante, LGTel) y la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSI), como leyes especiales, también otorgan competencias a la SGID para aplicar los procedimientos dispuestos en el Título VIII. Al margen de estas dos normas, se han aprobado en los últimos años diversas leyes que también facultan a la Agencia y, en particular, a la SGID, para intervenir controlando y supervisando la aplicación de determinadas disposiciones. Entre ellas, se encuentran la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, que tienen un impacto directo en la actividades de la SGID, la Ley Orgánica

10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, o la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual, por citar las más significativas. Como no puede ser de otra manera, estas nuevas asignaciones redundan en un incremento de la entrada, con reclamaciones que vienen de ámbitos normativos diferentes con peculiaridades propias que conviene distinguir a la hora de realizar los procedimientos.

En definitiva, todo ello contribuye a una tendencia de aumento de las reclamaciones y del trabajo de la Agencia que previsiblemente se continuará produciendo en los próximos años, por la persistencia de las causas que lo producen, y como se deduce claramente del estudio del marco temporal 2007-2022 presentado anteriormente, poniendo el foco sobre los organismos de control y los recursos disponibles para atender todas las reclamaciones recibidas. En este sentido, también conviene destacar el aumento del 13% de los recursos de reposición interpuestos contra resoluciones de los procedimientos, después de haber aumentado también el año anterior de forma importante (un 18%), lo que supone un incremento de 31% en dos años.

Analizando ahora los actos finalizadores de las actuaciones de la SGID, lo primero que se debe destacar es que el 60% de las reclamaciones recibidas finalizan tras el análisis previo de admisibilidad y, por lo tanto, no prosiguen a fases posteriores.

Hay que destacar, la excepcionalidad del procedimiento sancionador, por lo que, cuando sea posible, se opta por mecanismos alternativos amparados por la normativa, tal y como ocurre con la remisión de la reclamación al DPD o al responsable o encargado, según dispone el artículo 65.4 de la LOPDGDD. Tomando como referencia las reclamaciones que superan el análisis previo de reclamación, es decir, el 40% de las reclamaciones, se observa que solo el 11% de las resoluciones se producen en el procedimiento sancionador, frente al 79% que se producen tras el traslado de la reclamación. La principal vía de resolución de reclamaciones pasa por su remisión al responsable o encargado del tratamiento, que analiza la reclamación y proporciona una respuesta a la Agencia que, en un número significativo de casos, permite concluir que no existe infracción o que esta ha sido corregida, por lo que no procede continuar con las actuaciones.

Estos mecanismos también tienen reflejo sobre los tiempos en que los ciudadanos obtienen respuesta a sus reclamaciones. En este año, el tiempo medio de resolución de las reclamaciones que superan el análisis previo de admisibilidad se ha reducido un 9%. Además, las reclamaciones que se resuelven tras el traslado de la reclamación permiten que los ciudadanos vean satisfechos sus intereses en un plazo inferior a los tres meses, lo que supone un importante logro frente a la tramitación tradicional.

Del análisis de los datos por grupos de clasificación, se observa un año más cómo las reclamaciones más frecuentes son las relacionadas con servicios de internet, videovigilancia y publicidad (suman un 42% entre los tres grupos), con un aumento muy destacado en estas últimas, que crecen un 31%. En relación con ello, a final de año se ha trabajado en la modificación del código de conducta publicitario de Autocontrol, al que se han podido adherir al comienzo ya de 2023 los principales operadores de telecomunicación, para la intermediación y rápida resolución de las reclamaciones sobre publicidad no deseada, mecanismo que ya en febrero de 2023 se encuentra operativo. También destaca el importante aumento de las reclamaciones recibidas sobre comercio, transporte y hostelería (+34%) y, dentro de este ámbito, el aumento de infracciones reclamadas relacionadas con el uso de datos personales por parte de empresas de reparto y paquetería; durante el año 2022 se ha producido un aumento de las reclamaciones asociadas a la entrega de paquetería donde aparecen los datos personales de los destinatarios a vecinos o tiendas cercanas. Por último, cabe reseñar un aumento también relevante (+23%) en reclamaciones sobre contratación fraudulenta, que atañen principalmente a los sectores energético y de telecomunicaciones.

En relación con los procedimientos sancionadores y las multas, el ámbito más frecuente de los primeros es la videovigilancia (164 proce-

dimientos), sin embargo, el mayor volumen de multas corresponde a los casos relacionados con servicios de Internet. Esto se explica por la, generalmente, menor entidad de los casos de videovigilancia, tanto por su gravedad como por el tipo de responsable (personas físicas) y su relación con la eficacia de las multas (en términos de proporcionalidad y capacidad de disuasión), frente a la gran repercusión de las infracciones en el ámbito de Internet y la presencia de grandes compañías en ese ámbito. Así, la mayor multa impuesta en el año se corresponde con un procedimiento de este sector, en el que se impone a Google LLC, por infracción de los artículos 6 y 17 del RGPD, una multa de 10 millones de euros, además de ordenar las medidas necesarias para corregir la infracción e impedir su reproducción en el futuro, como se detallará en el siguiente apartado.

Observando los grupos de clasificación en términos del volumen de multas impuestos, también destaca un descenso destacado (-90%) en el importe de las multas del grupo de telecomunicaciones, lo que se explica por los procedimientos resueltos el año anterior con importantes multas, relativos a los duplicados de tarjetas SIM realizados de manera fraudulenta.

En el ámbito europeo, dentro de los mecanismos de cooperación entre las autoridades de control de los Estados del Espacio Económico Europeo (EEE) para la gestión de los casos transfronterizos, se ha observado un aumento en la recepción de nuevos casos transfronterizos procedentes de otras autoridades europeas (+12%), así como del número de decisiones de procedimientos participados por la Agencia (+17%), el paso final de un proceso complejo de consenso y resolución que puede durar varios años. En este sentido, la SGID ha participado en varios grupos de trabajo europeos para cohesionar criterios y cooperar en diversas materias, como se detalla en el apartado de “Memoria en cifras”.

Asimismo, hay que citar también las obligaciones que tiene la SGID en relación con la supervisión de la protección de datos personales de las diversas agencias de la Unión Europea y de sus grandes sistemas de información, que sirven a las finalidades de cooperación entre los EEMM, en particular en el ámbito judicial, policial, y de control de aduanas y fronteras. Las normas de protección de datos propias de cada uno de ellos se encuentran primariamente en sus respectivas normas de establecimiento, que normalmente tienen la forma de Reglamento UE, sin perjuicio de que sean también de aplicación, dependiendo del ámbito material en que opera la agencia o sistema, el Reglamento General de Protección de Datos (RGPD) y la Directiva de Ámbito Penal (DAP). Las auditorías a estos grandes sistemas se están implantando gradualmente y, aunque el plazo de cada una puede diferir entre tres o cuatros años para finalizarlas, su evaluación se realiza de manera continua.

Durante 2022, se han desarrollado las auditorías del Sistema de Información de Visados (VIS) y del Sistema de Información Schengen (SIS II). En este contexto, se han mantenido reuniones de coordinación de SIS II con las autoridades nacionales SIS II en el marco de la planificación de la evaluación Schengen 2021-2025. Y en el ámbito de las evaluaciones Schengen 2021-2025, se han celebrado las reuniones de seguimiento correspondientes a VIS y SIS II (oficina SIRENE) para evaluar los resultados del informe de evaluación, las medidas a adoptar por las autoridades y el calendario de implementación.

Finalmente, entre los resultados anuales se debe hacer referencia al canal prioritario de la Agencia para solicitar la retirada urgente de contenidos sexuales o violentos publicados en Internet sin consentimiento. El total de casos tramitados por vía urgente tras el análisis de la Agencia creció un 107% en el año y la eficacia de las intervenciones para lograr la retirada de contenidos fue del 90%. La principal dificultad que se enfrenta para lograr la supresión es la identificación o respuesta satisfactoria por parte de responsables que se encuentran establecidos en terceros países fuera de la UE.

El detalle completo del volumen de trámites realizados por la Subdirección General de Inspección de Datos y su valoración se ha incluido en el apartado de esta memoria correspondiente a la “Memoria en cifras”.

Con objeto de gestionar el aumento en la carga de trabajo que tiene que soportar el personal de la SGID, durante el año 2022 se ha continuado trabajando sobre los tres ejes identificados: simplificación y automatización, modificaciones normativas, y adecuación de la plantilla.

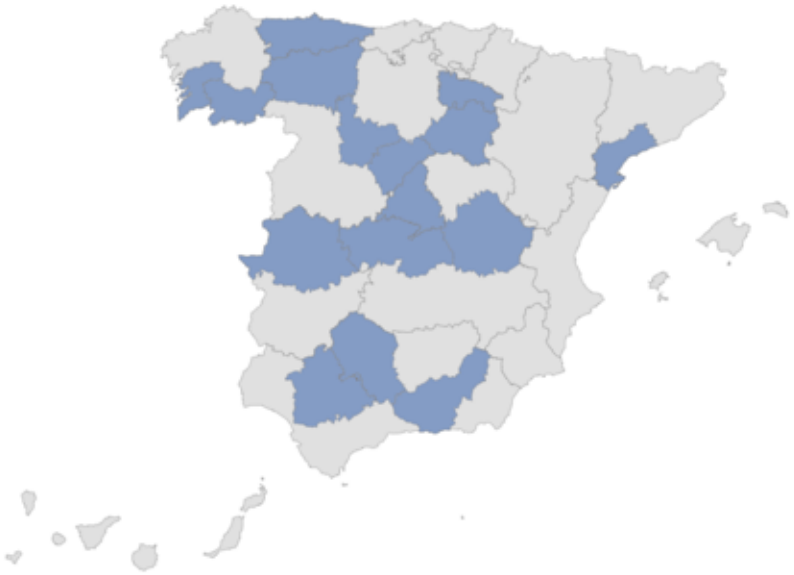
En el primer eje, se ha añadido automatización en diversos pasos de los procedimientos de la SGID, tanto basada en sistemas de información, como en modelado de documentos dinámicos, con el objeto de reducir los tiempos de tramitación. Así, el tiempo medio de tramitación de las primeras fases del proceso de respuesta a reclamaciones, donde se ha podido añadir mayores niveles de automatización, se ha reducido entre un 2% para las actuaciones de traslado de reclamación y las actuaciones previas de investigación y un 9% para el análisis previo de admisibilidad. También se han evaluado procesos de robotización y técnicas basadas en inteligencia artificial para su futura incorporación en distintas tareas auxiliares a los procedimientos. Todo esto redunda en mejoras para los ciudadanos que ven resueltas sus reclamaciones en menor tiempo.

En relación con las modificaciones normativas, se ha impulsado la aprobación de las modificaciones a la LOPDGDD, que puedan dar mejor cobertura a los procedimientos de respuestas a las reclamaciones y que simplifiquen y mejoren los tiempos de respuesta conservando todas las garantías procedimentales.

Por último, en cuanto a la adecuación de la plantilla, se ha producido un incremento de diez puestos adicionales en la RPT. Este incremento de puestos se ha debido al aumento de las competencias que se han ido adquiriendo en los últimos años que fue la causa de que en 2021 se identificara el número de trabajadores que debía tener la SGID para poder atender las diferentes actividades a realizar. Como consecuencia de ello, se estableció un plan a varios años vista para poder adecuar la estructura al trabajo que se debe elaborar que seguirá pendiente en futuros ejercicios.

Gracias a este incremento en los puestos de trabajo y a poder cubrir algunas plazas vacantes la plantilla efectiva ha aumentado en catorce personas Este talento especializado se ha podido atraer en cierta medida gracias al avanzado programa de teletrabajo con que cuenta la Agencia, que permite incorporar a personas que residen en comunidades autónomas distintas a donde se encuentra ubicada la sede de la Agencia. Así, en la actualidad, la SGID cuenta con una cuarta parte de la plantilla que reside y trabaja de forma habitual fuera de Madrid, como se muestra en la siguiente figura.

Lugar de residencia y trabajo del personal de la SGID



Todas las nuevas incorporaciones han recibido una formación introductoria de dos meses para el desarrollo de su trabajo, además del propio plan de formación anual de la Agencia, que entre otros cursos especializados, incluye la posibilidad de sufragar con cargo al mismo la asistencia a actividades formativas externas en materias específicas relacionadas con el adecuado desempeño de los puestos de trabajo, lo que incluye la financiación del Máster en el Reglamento General de Protección de Datos impartido por la UNED.

En relación con este aspecto hay que destacar que se ha cambiado la estructura de la Subdirección para separar la parte de Inspección de la de Instrucción, teniendo, por lo tanto, un área diferente para cada una de las funciones establecidas en la normativa para la tramitación de la reclamación: dos para la evaluación previa de admisibilidad, otras dos para las actuaciones después de la admisión a trámite y una última para los recursos y las actuaciones transversales.

5.2. Reclamaciones y procedimientos más relevantes

En el año 2022 se han afianzado las reclamaciones relacionadas con la promoción publicitaria, suponiendo un 13% del total de reclamaciones recibidas. Esto supone el tercer lugar en cuanto al grupo de actividad principal de las reclamaciones.

De todas estas, una mayoría hace referencia a la recepción de llamadas telefónicas comerciales no deseadas. Pero también hay casos destacades de envíos de publicidad por vía postal. Es el caso del **PS/00508/2022** contra FACTOR ENERGÍA, S.A. en el que se sanciona con 40.000€ por el envío de publicidad sin base de legitimación. La entidad manifiesta que los datos proceden de fuentes de acceso público, pero no lo acredita, y realiza una ponderación que se considera insuficiente para justificar la prevalencia del interés legítimo.

A pesar del aumento en los dos últimos años de las reclamaciones por publicidad, por encima siguen estando las relacionadas con servicios de Internet. De todos los procedimientos sancionadores abiertos y resueltos en el año en curso, cabe destacar por la cuantía de la multa administrativa el **PS/00140/2020** contra Google LLC con un importe de 10.000.000 €.

En este procedimiento se denunció que Google hacía cesión de datos personales a terceros de forma fraudulenta, en este caso a la base de datos Lumen Database. El proyecto Lumen tiene por misión la recogida y puesta a disposición, tanto de investigadores como de personas interesadas, de solicitudes de retirada de contenido de páginas web de dentro y fuera de Estados Unidos, en abierto. GOOGLE LLC comunica al "Proyecto Lumen" toda la información correspondiente a estas solicitudes de ejercicio del derecho al olvido, incluida la identificación del solicitante y el afectado, en su caso, su dirección de correo electrónico, los motivos que se alegan (el texto de la reclamación) y la URL reclamada, así como la documentación que sirve de soporte, si existe.

Asimismo, la Política de Privacidad de Google LLC no hace referencia ni contiene ningún enlace que conduzca a un formulario específico de ejercicio de derechos en materia de protección de datos personales. En los casos de retiradas de contenidos de productos y servicios analizados es difícil deducir si la solicitud se formula invocando la normativa de protección de datos personales, sencillamente porque esta normativa no se menciona en ninguno de los formularios, con independencia del motivo que el interesado seleccione de entre las opciones propuestas, salvo en el formulario denominado "Retirada en virtud de la ley de privacidad de la UE", el único disponible que contiene una referencia expresa a esta normativa. El sistema diseñado por GOOGLE LLC, que conduce al interesado a través de diversas páginas para llegar a cumplimentar su solicitud obligándole previamente a marcar las opciones que se ofrecen, puede provocar que este termine marcando una opción que se adapte a los motivos que considera apropiados a su interés, pero que le aparta de su intención originaria, que puede estar claramente vinculada a la protección de sus datos personales, desconociendo que estas opciones le sitúan en un régimen normativo distinto porque

así lo ha querido GOOGLE LLC o que su solicitud se resolverá según las políticas internas establecidas por esta misma entidad.

Además, presentada la solicitud de retirada de contenido en línea y atendido el derecho, es decir, acordada la supresión de los datos personales, no cabe un tratamiento posterior de los mismos, como es la comunicación que GOOGLE LLC realiza al "Proyecto Lumen".

Por todo ello, se impuso una multa de 5.000.000€ por la infracción del artículo 6 del RGPD; y 5.000.000€ por la infracción del artículo 17.

También se puede destacar el procedimiento de derechos **PD/00146/2022** contra Google, en el que se estima la reclamación que solicita de nuevo el derecho al olvido de una URL. Google afirma que ha obtenido esta URL de una publicación actual sobre el comportamiento profesional del reclamante. La URL, además de las noticias que hacen referencia a presuntos delitos, información que estaría protegida por el derecho a la libertad de información, también contiene una fotografía del NIE del reclamante. Es este detalle el que hace que se estime la reclamación, ya que no está justificada la publicación de documentos personales.

Con relación al derecho al olvido y a la publicación de documentos personales se resolvió el **PS/00485/2021** contra un particular que publicó en internet el DNI de uno de los reclamantes, que iba incluido en la demanda judicial que interpusieron los reclamantes al particular y que publicó íntegra en Internet. Se multa con 5.000€ por la infracción del artículo 5.1.c del RGPD.

De mayor importe es la multa impuesta a Orange Espagne SAU en el **PS/00413/2021** por la imposición a las empresas de mensajería de realizar una fotografía del anverso y del reverso del DNI de los destinatarios cuando realizan una entrega. Si bien es lícito el tratamiento de imágenes para la contratación a distancia de un producto, no debe confundirse esto con la entrega del producto en sí a su destinatario. La comprobación del DNI en tiempo real podía realizarse a través de otros medios disponibles por Orange sin la necesidad de obtener una copia del DNI. Se finaliza el procedimiento con multa de 100.000€ por infracción del artículo 5.1.c del RGPD

Siguiendo con los operadores de telecomunicación, se instruyeron los procedimientos sancionadores **PS/00281/2021** y **PS/00340/2021** contra VODAFONE ESPAÑA, S.A.U. por el alta de dos líneas SIM vinculadas a los datos personales de los reclamantes sin su consentimiento. En el primero se impuso una multa de 100.000€ por no atender el derecho de acceso y otros 100.000€ por no atender el de supresión. Además, se sancionó con otros 70.000€ por el alta de la línea en la que se consultó ASNEF, sistema de información de solvencia, aunque a través de otra empresa.

En el segundo procedimiento, en el que la reclamada fue citada por la Guardia Civil en calidad de investigada en relación con las estafas cometidas con la línea dada de alta a su nombre, se impuso una multa de 100.000€

En cuanto al número de reclamaciones recibidas relacionadas con los servicios de Internet, detrás de los buscadores aparecen las redes sociales. En este sector son destacables los expedientes abiertos por la grabación y publicación sin consentimiento de imágenes, vídeos u otros contenidos audiovisuales como audios.

De esta manera, cabe destacar en el año 2022 que se han dictado trece procedimientos sancionadores contra diversos medios de comunicación. Nos referimos al **PS/00158/2022** contra 20 Minutos Editora, S.L., **PS/00190/2022** contra Atresmedia Corporación de Medios de Comunicación, S.A., **PS/00191/2022** contra Conecta5 Telecinco, S.A.U., **PS/000192/2022** contra Corporación de Radio y Televisión Española S.A., **PS/00193/2022** contra Diario ABC, S.L., **PS/00194/2022** contra Display Conect, **PS/00195/2022** contra Editorial Prensa Canaria, S.A., **PS/00196/2022** contra El Diario de Prensa Digital, S.L., **PS/00197/2022** contra La Vanguardia Ediciones, S.L., **PS/00198/2022** contra El Diario de Prensa Digital, S.L., **PS/00199/2022** contra Sociedad Española de Radiodifusión, S.L., **PS/00200/2022** contra Titania Compañía Editorial, S.L. y **PS/00201/2022** contra Unidad Editorial Información General S.L.U.

Estos medios de comunicación publicaron en sus sitios web el audio de la declaración ante el juez de una víctima de una violación múltiple, para ilustrar la noticia relativa a la celebración del juicio en un caso que muy mediático. La voz de la víctima se podía oír perfectamente sin distorsionar.

Partiendo del hecho indubitado de que la voz es un dato de carácter personal, y sin perjuicio del respeto pleno al Derecho Fundamental a la Libertad de Información, los medios de comunicación cuando actúan como responsables del tratamiento están obligados a cumplir con el RGPD y la LOPDGDD.

Precisamente porque no se niega el evidente interés público informativo en la noticia, dado el interés general en las causas penales, en este caso concreto, no se trata de hacer decaer el Derecho Fundamental a la Libertad de Información por la prevalencia del Derecho Fundamental a la Protección de Datos de Carácter Personal, sino de hacerlos plenamente compatibles para que ambos queden absolutamente garantizados. Esto es, no se pone en cuestión la libertad de información de los medios de comunicación sino la ponderación con el derecho a la protección de datos en base a la proporcionalidad y necesidad de publicar el concreto dato personal de la voz en atención al riesgo en los derechos y libertades de la víctima.

Tal situación podría haberse resuelto con la utilización de procedimientos técnicos para impedir el reconocimiento de la voz, tales como, por ejemplo, la distorsión de la voz de la víctima o la transcripción del relato de la violación múltiple, medidas de seguridad ambas, aplicadas dependiendo del caso de forma ordinaria por los medios de comunicación.

Significar que en todos ellos se adoptó previamente una medida provisional de retirada del contenido conforme previene el artículo 69 de la LOPDGDD, a los efectos de salvaguardar el Derecho a la Protección de Datos de Carácter Personal de la víctima.

Se sanciona a cada uno de ellos por una infracción del artículo 5.1.c) de RGPD con una multa de 50.000 euros.

En la misma línea se encuentra el **PS/00327/2021** contra una particular que grabó a unos niños denigrando a otro de ellos. La directora del colegio donde estudian estos niños denunció este caso a la Guardia Civil y a la Agencia. El juzgado terminó archivando la causa al no aparecer debidamente justificada la perpetración del delito que lo motivó. En relación con la infracción administrativa, se impuso una medida cautelar de retirada en el inicio del procedimiento sancionador y posteriormente se terminó sancionando el tratamiento de los datos sin la legitimación con una multa de 10.000€ por infracción del artículo 6 del RGPD.

Con la misma temática se firmó la resolución **RR/00342/2022** desestimatoria del recurso presentado por la petición de retirada de contenidos en una medida cautelar que se realizó para que una persona particular retirara un vídeo de las menores de Burjasot presuntamente violadas. Este caso se trata del primer recurso que ha llegado contra una medida cautelar.

Siguiendo con los servicios de Internet, hay dos casos contra páginas web de contenidos pornográficos que se deben mencionar. El **PS/00554/2021** contra BURWEBS S.L. y el **PS/555/2021** contra TECHPUMP SOLUTIONS S.L., ambas entidades titulares de una y cinco páginas web respectivamente, dedicadas a la pornografía.

Destacaremos, respecto de estos procedimientos sancionadores que, en el caso de las webs dedicadas a la pornografía titularidad de las empresas sancionadas, existía un riesgo cierto de que los menores de edad accedieran directamente y sin limitaciones a un contenido perjudicial para ellos: el acceso indiscriminado de los menores a la pornografía en internet constituye un alto riesgo en sus derechos y libertades.

Así, las limitaciones o cautelas previstas en las páginas web resultaban claramente insuficientes para evitar el acceso a los menores, tanto de forma directa a la página web (usuarios no registrados), como en aquellos supuestos en los que era preciso

un registro (usuarios registrados). Si bien había presentes mecanismos para "declarar" la edad, no existía ninguno para comprobarla ulteriormente, ni ninguno para verificarla ab initio.

Y es que, los riesgos a los que están afectos los menores, inherentes a su desarrollo, han de ser considerados por los responsables del tratamiento, y no sólo por aquellos que dirigen servicios directa y específicamente a los niños, sino por todos aquellos que realizan tratamientos de datos personales dirigidos a otros colectivos en los que los menores puedan interactuar o intervenir (en una sociedad cada vez más tecnológica) y ver en riesgo su integridad física o psicológica y comprometidos sus derechos y libertades como sucede con la pornografía en internet.

Resultando que estas entidades deciden que las categorías de interesados se limitan a los mayores de edad, les corresponde implementar las medidas técnicas y organizativas apropiadas para que el tratamiento se efectúe únicamente respecto de interesados mayores de edad. Ello conlleva que también implemente las medidas técnicas y organizativas apropiadas para que los datos de los menores de edad no sean tratados.

En atención a todo lo antedicho, se ordenó a las entidades citadas que adecuaran el tratamiento de sus datos personales al RGPD, adoptando medidas de seguridad apropiadas mediante las que se verificase la edad de los usuarios, registrados o no, que accedan a las páginas web referenciadas, garantizando que son mayores de edad, impidiendo incidencias similares en un futuro.

Se sanciona a BURWEBS S.L. con una multa de 75.000 euros por una infracción de los artículos 5.1.a), b) y e), 8, 12.2, 13, 25 y 30 del RGPD y del artículo 22.2 de la LSSI.

Y se sanciona a TECHPUMP SOLUTIONS S.L. con una multa de 525.000 euros por una infracción de los artículos 5.1.a), b) y e), 6.1, 8, 12.1, 12.2, 13, 25 y 30.1 del RGPD y del artículo 22.2 de la LSSI.

Otro caso de publicación de imágenes sensibles en webs de pornografía es el **AI/00314/2022** contra un responsable desconocido. Este mediático caso se inicia por una reclamación firmada por 21 mujeres que fueron grabadas con una cámara oculta mientras orinaban en la calle durante el transcurso de una romería popular celebrada en Galicia en julio de 2019. Las imágenes fueron publicadas en diversos sitios web de contenido pornográfico y de descarga de archivos. Los hechos fueron denunciados ante la Guardia Civil, acompañándose copia de las diligencias fruto de la labor investigadora realizada por la compañía de Burela (Lugo). Se comprobó que, en el momento de recibir la reclamación, permanecían disponibles en un enlace para descarga directa, y en un sitio web para usuarios registrados. Se ha conseguido eliminar lo publicado en el sitio de descargas, pero no se ha podido identificar al responsable del segundo sitio web que se encuentra fuera del Espacio Económico Europeo, no existiendo ninguna clase de texto legal identificativo, y haciendo caso omiso al requerimiento de información sobre las cuentas de los usuarios que los publicaron. No obstante, se consiguió que el vídeo fuera de acceso restringido.

Tampoco se pudo identificar al responsable en el **AI/00410/2022**. Este procedimiento se inició de oficio tras las denuncias recibidas en relación con la publicación en Twitter y Facebook de unos audios en relación con el caso Arandina, grabados por la menor objeto de abusos. Tras una larga investigación, no ha sido posible determinar a quien pertenecían las cuentas desde las que se publicaron los audios. Las publicaciones denunciadas que contenían el audio al que se hacía referencia en las denuncias han sido eliminadas de las direcciones informadas.

De datos de menores y contenido audiovisual trata el procedimiento sancionador **PS/00107/2022**. El origen de este expediente es una reclamación recibida por el canal prioritario, en la que el reclamante aporta copia de sentencia del Juzgado de Menores nº 1 de Murcia, por la que se impone al reclamado, con 16 años en la fecha de los hechos, una pena máxima de 4 meses de tareas socioeducativas, como autor de un delito de amenazas condicionales contra la hija del reclamante, con 13 años en dicha fecha.

De los hechos probados se desprende que el reclamado entabló relación estrecha con la menor a través de la red Instagram, llegando la menor a mandarle videos y fotos de carácter íntimo por la red Instagram o por Whatsapp. Ante la negativa de la menor a seguir enviando imágenes, el reclamado la amedrentó amenazándola con publicar las fotos de que disponía. Debido al temor producido, la menor envió los videos solicitados, hasta 10 en una misma noche, presionada por la amenaza de que su imagen se difundiera en redes y llegara a su pueblo y a sus conocidos. Se produce una infracción del artículo 6.1 y se impone una multa de 5.000 euros.

En el **PS/00418/2021** el reclamante manifiesta que el grupo municipal del Ayuntamiento de Madrid de VOX realizó una visita a las instalaciones del IES Ramiro de Maeztu apoyando el deporte base junto a la Directiva del Club de Baloncesto Estudiantes; en dicha visita se realizó un video de un minuto que se difundió en redes sociales, Twitter e Instagram; en el citado video aparecen menores sin que se haya consentido en el tratamiento de sus datos.

El reclamado señala que la información se refiere a un suceso o acontecimiento público y la imagen de los menores aparecen como meramente accesoria, sin que en ningún caso se produzca menoscabo de la honra o reputación de los menores. Aduce igualmente que su base jurídica legitimadora de los datos de los menores se encuentra en el artículo 25 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, por mor del art. 6.1.e) del RGPD.

En el este caso, si consideramos que el interés público invocado por el reclamado viene determinado por el mandato genérico establecido en las anteriores normas dirigido a las entidades locales para la promoción física y deportiva, de las instalaciones deportivas, así como la ocupación del tiempo libre, etc., el tratamiento llevado a cabo mediante la grabación de las imágenes de menores y su difusión en las redes sociales Twitter e Instagram a través del video realizado en las instalaciones del IES Ramiro de Maeztu no es necesario para el cumplimiento de esa misión de interés público, estimándose que vulnera el artículo 6.1 del RGPD. Además, en la norma invocada no se impone la obligación de dicho tratamiento, no se determina esa misión de interés público y no se confiere poder público para llevar a cabo el tratamiento.

De esta forma, en este caso concreto, la persona que es grabada tiene derecho a consentir sobre la recogida y uso de su imagen y, además, corresponde al responsable del tratamiento asegurarse de que aquel a quien se solicita su consentimiento efectivamente lo da.

Por tanto se produce una infracción artículo 6.1 RGPD, con sanción de apercibimiento y la adopción de medidas requiriendo al Grupo Municipal VOX Ayuntamiento de Madrid, para que en el plazo de un mes desde la notificación de esta resolución, acredite la adopción de medidas para que no vuelvan a producirse incidencias como la que dio lugar al procedimiento sancionador: la captación y difusión de imágenes de menores en un vídeo sin el consentimiento de sus progenitores y que los tratamientos efectuados se ajustan a las exigencias contempladas en el artículo 6.1 del RGPD y a suprimir la imagen de todos los menores que aparezcan en el vídeo que tienen publicado en redes sociales.

También sobre menores y su grabación en el entorno escolar es el **PS/00566/2021**. La policía local levanta acta a instancia del director de un CEIP, indicando que varios días antes, en su centro de educación infantil y primaria un individuo estuvo increpando y grabando a los alumnos mientras se encontraban realizando educación física en el patio. Además, expuso las imágenes captadas en su Facebook un breve espacio de tiempo.

Durante la fase de pruebas se aportó el perfil de Facebook del reclamado; en ese momento almacenaba dos videos. En el primero hay un periodo corto en que se ve claramente a los alumnos, enfoca a su cara, y aunque llevan mascarillas se les identifica. El reclamado increpa a los profesores y alecciona a los niños de que no se hiciera uso de las mascarillas en clase de educación física. En el segundo video sale solo una persona hablando sobre el asunto, persona a la que identifican los profesores, que es el reclamado, aludiendo a lo malo que será llevar mascarilla cuando se hace deporte.

Los videos se entregaron a la Policía que averiguó quien era el reclamado, figurando sus señas en el acta.

Se considera que, una vez cometida la infracción, el video conteniendo las imágenes se suprimió de su página de Facebook, sin que se extendieran los efectos de la infracción. Estuvo según indicadores de Facebook, 11 horas expuesto. Se sanciona por la infracción del art. 6.1 del RGPD con una multa de 3.000 euros

En el ámbito educativo y cultural hay algunos expedientes que merecen mención, como el **E/12222/2021** contra la Associació Plataforma per la Llengua. Se iniciaron actuaciones de investigación mediante acuerdo de la Directora que tuvo conocimiento como consecuencia de las dos denuncias recibidas sobre La Plataforma per la Llengua, la ANC y varios sindicatos estudiantiles como el Sindicat d'Estudiants dels Països Catalans (SEPC) que han lanzado una web para quejarse en relación con profesores universitarios que impartan las materias en castellano. La aplicación permite a los estudiantes de todas las universidades de Cataluña, Baleares y la Comunidad Valenciana denunciar "cambios de lengua" en las asignaturas que cursan. Es decir, permite señalar a aquellos profesores que, habiéndose comprometido a impartir la clase en catalán, saltan al castellano para dirigirse a un alumno que no le comprenda por proceder de otra comunidad autónoma o país.

Las entidades denunciantes añaden que en la web reclamada se recogen datos personales de terceros, vinculados a denuncias realizadas por sus usuarios, de profesores que, en las Universidades de Cataluña, Baleares y la Comunidad Valenciana, utilicen el castellano en las aulas.

Se archiva porque tras las actuaciones de investigación efectuadas, se ha comprobado que en el formulario de presentación de la queja no se solicitan los datos de los profesores concretos que imparten las clases en castellano; tampoco, dentro de los datos recopilados, la asignatura ni el horario concreto dentro de los estudios, por lo que no se aprecia que se imponga, de forma directa o indirecta la identificación, del profesor.
Existe un campo "Comentarios" en la que, no obstante lo anterior, podrían incluirse datos de terceros, aunque la plataforma denunciada advierte sobre que no se permiten los datos de terceros salvo autorización.

Ante la posibilidad de recibir algún dato personal de terceros mediante dicho campo libre de "Comentarios", han elaborado e implementado un procedimiento interno para evitar el tratamiento de dichos datos personales. Este procedimiento se incluye como parte del protocolo de tratamiento de datos que consiste en depurar por parte de la responsable del área Social de Plataforma por la Llengua las quejas recibidas revisando que no haya ningún tipo de información que haga referencia a información relativa a una tercera persona, o información contextual que pueda facilitar la identificación de una tercera persona concreta ("Datos de Terceros"). Si por error el reclamante ha añadido información de este tipo a la queja, ésta se marca para pedir inmediatamente su eliminación al gestor del almacenamiento.

Además, no se tiene evidencia de que este hecho se haya producido ni de que se haya realizado

tratamiento alguno con los datos de ningún profesor. Tampoco consta en esta Agencia ninguna reclamación presentada por un afectado a este respecto.

También cabe destacar las actuaciones de investigación **AI/00086/2022** contra la Universidad Internacional de la Rioja. La investigación se inicia a raíz de numerosas reclamaciones recibidas contra esta universidad por la información facilitada a los alumnos sobre el tratamiento de datos biométricos (mediante cámaras web) con la finalidad de confirmar su identidad en los exámenes telemáticos. A raíz de la investigación no se puede acreditar el tratamiento de datos biométricos. Por ello, se archiva el caso.

Contra otra universidad es el procedimiento de derechos **PD/00109/2022**. En él, el reclamante solicita a la Universidad Nacional de Educación a Distancia, UNED, la matrícula y las notas de estudio de su hija mayor de edad. Aporta sentencia judicial para la modificación de la pensión alimenticia, que estima su pretensión parcialmente, manteniendo la pensión de la hija condicionada a la matriculación y la aplicación a los estudios. El padre tiene derecho a los datos de la matrícula y notas de estudio y la hija se encuentra obligada a suministrarlo. Pero solicitado esto a la UNED, ésta lo deniega aduciendo falta de interés legítimo del progenitor.

Se examina si concurre el interés legítimo y entre otras cuestiones se precisa que, aunque una sentencia judicial imponga a la hija del reclamante la obligación de suministrar a su progenitor determinados datos académicos no obsta para que el progenitor pueda reclamar al responsable del tratamiento tales datos amparándose en su interés legítimo, ni que por existir tal pronunciamiento judicial o porque la hija haya podido informar al padre al respecto o tenga intención de hacerlo, el responsable del tratamiento se vea imposibilitado a suministrarlos cuando aquel interés legítimo concurra.

Sin embargo, se estima puesto que, examinada la documentación obrante en el expediente, aportada por las partes durante su tramitación, cabe concluir que concurre un interés legítimo de la parte reclamante para obtener información relativa a la matrícula y notas de estudio, siempre en el bien entendido de que dicha finalidad será exclusivamente la de utilizarlas en el procedimiento judicial para la solicitud de modificación de la pensión asignada.

En el ámbito sanitario hay varios procedimientos reseñables. Entre ellos, está el **PS/00132/2021** en el que se sanciona con apercibimiento a la Consejería de Sanidad Canaria por no haber nombrado DPD desde la aplicación del reglamento. No obstante, lo ha nombrado a lo largo del procedimiento sancionador.

También contra este mismo organismo (Consejería de Sanidad Canaria) se instruyó el **PS/00411/2021** iniciado por una reclamación de un particular frente a Acuerdo del Consejo de Gobierno Canario por el establecimiento de un registro de datos de clientes de hostelería en el que requiere la aportación de datos excesivos y no se informa debidamente de los derechos que asisten a los afectados. Se sanciona con un apercibimiento por la infracción del artículo 5.1.c del RGPD ya que los datos recolectados son excesivos para el objeto de localizar a un contacto y realizar un rastreo por COVID-19. Este criterio, junto con el de la anonimización de los titulares del dispositivo, ha sido el asumido por el Comité Europeo de Protección de Datos en las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo.

El **PS/00222/2021** apercibe a la Secretaría de Estado de Digitalización e Inteligencia Artificial, SEDIA, con relación a la aplicación móvil que permitirá el rastreo de contactos por Bluetooth con objeto de la detección precoz de posibles contagiados por la COVID-19 (Radar COVID). Las infracciones hacen referencia a los artículos del RGPD 5.1.a) y 5.2; 12 y 13; 25; 28.3; 28.10; y 35. La SEDIA ha actuado como responsable del tratamiento, so pena de no ostentar las competencias para ello ni ser designada a tales efectos por la Dirección General de Salud Pública.

Y sobre este mismo tema trata el **PS/00233/2021**, también relacionado con la misma aplicación

RADARCOVID: se impone a la DIRECCIÓN GENERAL DE SALUD PÚBLICA la sanción de apercibimiento por infracción de los siguientes artículos: 5.1.a) y 5.2; 12 y 13; 25; 28.1 y 28.3 y 35 del RGPD. En este caso, la Dirección General de Salud Pública, siendo responsable del tratamiento conforme a las competencias que tenían atribuidas por mor de la normativa, no cumplió con las obligaciones impuestas por la normativa de protección de datos.

También sobre la COVID-19 se tramitó el **PS/00364/2021** contra el Ayuntamiento de Calpe. Una empleada de servicios sociales del Ayuntamiento de Calpe reclama contra los Laboratorios González SL (LAB) que le hicieron unos análisis para detectar anticuerpos COVID- 19. La prueba, promovida por el Ayuntamiento tenía carácter voluntario, y la reclamante reconoce que dio el consentimiento para hacérsela. Los resultados de los análisis íntegros se enviaron a la reclamante y a la concejal de servicios sociales. A raíz de las investigaciones realizadas se detecta que las condiciones del contrato firmado entre LAB y el Ayuntamiento recogen que el trabajador debe saber que el laboratorio enviará una copia de la analítica a la dirección de la empresa y que, si algún trabajador no está de acuerdo, lo debe comunicar en el momento de la extracción de sangre. Sin embargo, los trabajadores no fueron informados de ello. Se ceden unos datos de salud vulnerando el artículo 9.2.a del RGPD en cuanto a que el mismo ayuntamiento lo permite y una infracción del artículo 25 RGPD.

El **PS/00323/2021** es similar al anterior, pero contra los Laboratorios González SL (LAB), esta vez por una infracción del artículo 5.1.f) y se impone una multa de 20.000 euros.

Otro caso relacionado con la historia clínica es el **PS/00587/2021** contra la Consejería de Sanidad de la Comunidad de Madrid. En él se apercibe a la misma por un acceso indebido a una historia clínica producido en el Hospital de La Paz. El expediente se zanjó con resolución de apercibimiento y medidas para el organismo investigado por infracción de los artículos 5.1.f y 32 del RGPD, es decir, por una brecha de datos personales de confidencialidad y por falta de medidas de seguridad respectivamente.

Similar es el caso del procedimiento sancionador **PS/00033/2022** contra la Consejería de Sanidad de la Comunidad de Madrid en el que, en contestación a una queja interpuesta ante el Servicio de Atención al Paciente del hospital del sistema sanitario público, la reclamante recibió respuesta a la que se adjuntaba informe médico relativo a una tercera persona. Durante el proceso se alega fundamentalmente que se trata de un error humano. Se sanciona con apercibimiento por la infracción de los artículos 5.1.f) y 32.1 del RGPD.

Al margen de la sanidad, pero también por falta de medidas de seguridad se instruyó el expediente al que pertenece el procedimiento sancionador **PS/00626/2014** contra el Sindicato de Policías de Cataluña. Esta entidad sufrió un ciberataque en octubre de 2013 sobre su sistema de información que derivó en la publicación de los datos extraídos por parte de Anonymous. El expediente estuvo suspendido hasta el 03/12/2021). El importe de la multa asciende a 40.001€, el mínimo establecido para las infracciones graves en la LOPD, por la infracción de su artículo 9.

También por una brecha de datos personales se iniciaron mediante nota interior de la directora de la Agencia actuaciones previas de investigación (**E/07901/2021**) para averiguar lo acaecido en el Ministerio de Trabajo y Economía Social tras el ataque informático del que fueron víctimas. Finalmente se archivó el caso por considerar que no existió infracción de la normativa de la protección de datos tras examinar los artículos 32 y 33: las medidas con las que contaba el Ministerio eran suficientes y el ataque fue altamente complejo y efectuado con herramientas de difícil detección por los sistemas tradicionales de defensa.

Uno de los casos más destacados en materia de brechas de datos personales es el **PS/00572/2021** contra OUTENUVE, SL por una brecha de disponibilidad. La empresa se dedica al cloud computing y es encargada y subencargada en el tratamiento. Un ataque de ransomware cifró datos personales de unos 200.000 afectados, incluyendo datos de salud. Muchos de esos datos se perdieron definitivamente. Respecto de las medidas de seguridad relativas a la protección de datos, tenían imple-

mentadas medidas de seguridad adecuadas para determinados clientes, por lo que el ataque podía haber sido evitado si las hubieran tenido todos. Se resuelve con infracción del art. 28 del RGPD por no tener suscritos los contratos de encargo (multa de 50.000€); art. 32 por no acreditadas medidas de seguridad adecuadas para todos los clientes con una multa de 100.000€; y art. 37 por no tener designado un DPD con una multa de otros 50.000€. En total 200.000€.

Por terminar con las quiebras de datos personales, también es destacable el caso del Ayuntamiento de Sabiñánigo en el que se inició el procedimiento sancionador **PS/00058/2022** con resultado de apercibimiento. En este caso el encuentro de una memoria USB extraviada con información únicamente accesible por el jefe de la policía local (datos de condenas e infracciones) llevó a descubrir que no existe un control adecuado de autorizados ni de los accesos a los datos. Se declara infracción del artículo 9 de la LOPD sobre la seguridad de los datos y se apercibe al ayuntamiento.

Y es que la Administración Pública también es objeto de investigaciones y sanciones de apercibimiento. El **PS/00432/2020** contra el Consejo General del Poder Judicial se inició a raíz de una reclamación en relación con datos del reclamante que constaban en la página web del CGPJ. Tras manifestar que se habían eliminado, se pudo constatar que en realidad seguían publicados, lo que dio lugar a un apercibimiento por vulneración del artículo 32 del RGPD.

También en el ámbito de la Justicia se abrió el **PS/00046/2022** contra el Ministerio de Justicia por la publicación en su web de listas de admitidos y excluidos en unas oposiciones sin ocultar el número completo del DNI. Aunque esta reclamación se inadmitió inicialmente, finalmente se abrió un procedimiento sancionador por haber una sentencia judicial que otorgaba indemnización al reclamante precisamente por haberse publicado los datos.

El **PS/00297/2021** contra el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación apercibe a este organismo por vulneración del artículo 21 del RGPD al no existir un contrato con el encargado del tratamiento (Movistar y Orange) del servicio "España contigo" a través del cual se comunica los números de embajadas y consulados españoles cuando una persona viaja al extranjero. El expediente no cuestiona el interés público que tiene este servicio.

También por carecer de contrato con el encargado se apercibe al Centro de Investigaciones Sociológicas quien comenzó a realizar encuestas sociológicas durante el mes de abril de 2020. Así se recoge en el procedimiento sancionador **PS/00162/2021**.

En el **PS/00509/2021** se apercibe a la Dirección General de la Policía por la realización de fotografías de documentos de identificación mediante dispositivos móviles personales de los agentes durante la etapa de confinamiento debido a la COVID r. La situación especial en la que se encontraban los agentes, y el resto de la ciudadanía, hizo que en este caso particular y debido a las circunstancias que lo rodeaban se considerara una infracción del artículo 32.1 del RGPD al no contar los dispositivos personales con las medidas de seguridad necesarias para salvaguardar la información capturada.

También contra el mismo organismo se ha iniciado acto de apertura del procedimiento sancionador **PS/00480/2022**. En la cafetería de la Comisaría de Policía de San Sebastián se utilizan hojas en las que figuran datos personales tanto de policías destinados en dicha unidad, como de personas que han acudido a la misma a solicitar un DNI o un Pasaporte con la finalidad de aprovechar el papel. Los datos proceden de la oficina de expedición del Documento Nacional de Identidad de la Comisaría Provincial de Guipúzcoa. La brecha de datos personales, por tanto, no se ha producido en tratamientos con fines policiales por lo que resulta de aplicación el RGPD. Se sanciona por infracciones del art. 5.1.f) y 32 del RGPD con apercibimiento.

También con el foco en la Administración está la inadmisión a trámite **IT/04563/2022** de la denuncia presentada por la presidenta del Parlamento de Cataluña con motivo del programa Pegasus. En la denuncia se pone de manifiesto

que, entre los años 2015 y 2020, diversas personalidades del ámbito civil y de la política de Cataluña, entre ellas, miembros del Parlamento de Cataluña, habrían sufrido intromisiones en sus dispositivos electrónicos mediante este programa. Se inadmite la denuncia al no ser competente la AEPD para conocer los hechos que se ponen de manifiesto, dado que se refieren a actuaciones supuestamente realizadas por el CNI que constituyen materia clasificada y por tanto excluidas de la LOPDGDD y de la Ley Orgánica 7/2021.

Mismo desenlace tuvo el recurso extraordinario de revisión **RV/00006/2022** contra la resolución de la Agencia de un abogado representante de 33 magistrados catalanes con relación a la publicación de sus datos personales en el diario La Razón en marzo de 2014. La reclamación inicial se dirigía contra el Ministerio del Interior, así como contra el diario La Razón. La sentencia del Tribunal Europeo de Derechos Humanos y la publicación de una noticia en el diario El País que incluía un audio sobre una conversación entre varias personas del CNP dan motivo para la presentación de dos escritos solicitando la reapertura de uno de los expedientes que tratan este caso (**E/01860/2015**). Sin embargo, además de que los hechos ya están prescritos, están pendientes de decisión judicial, por lo que sobre la base al art. 126.1 LPACAP, se inadmite el recurso extraordinario de revisión interpuesto.

El **PS/00267/2020** contra Amazon Road Transport Spain SL es de los de mayor cuantía en su sanción en este año 2022. El procedimiento se cerró con una multa de 2.000.000€ por infracción del artículo 6 del RGPD. La empresa solicitaba el certificado de antecedentes penales a los transportistas autónomos que pretendían suscribir un contrato mercantil para trabajar con ellos, además de la solicitud de consentimiento en el contrato para realizar transferencias internacionales y de la solicitud en el trámite de verificación de antecedentes para que dos empresas (radicadas fuera del EEE) trataran sus datos. Adicionalmente, se requiere a la empresa para que, en el plazo de un mes, adecúe a la normativa de protección de datos personales las operaciones de tratamiento que realiza y la información que facilita a los interesados.

En la misma categoría de asuntos laborales se encuentra el **PS/00218/2021**. En este caso la empresa reclamada, Entidad Urbanística Colaboradora de Conservación Eurovillas, implantó un sistema de reconocimiento facial para el control diario de la jornada laboral bajo el pretexto de la situación de pandemia y para que los trabajadores no tuvieran que "tocar nada". Se sanciona con apercibimiento y se deja de utilizar dicho sistema.

Por finalizar la temática de asuntos laborales y los sistemas de control horario basados en datos biométricos, también se tramitó el **PS/00052/2021** contra el "Consorcio para la Construcción, Equipamiento y Explotación de la Sede Española de la Fuente Europea de Neutrones por Espalación" que implantó un sistema de huella dactilar para el control horario. Se apercibe al consorcio público por la infracción del artículo 35 del RGPD al no contar con una evaluación de impacto de protección de datos.

El **PS/00267/2021** contra Mercadona terminó con una sanción económica de 100.000€ por la infracción del artículo 12 y 6 del RGPD. La reclamante sufrió un accidente en uno de los establecimientos y realizó el ejercicio del derecho de acceso de las imágenes de videovigilancia, el cual no fue atendido. Por tanto, se dejó de atender el derecho de acceso, por un lado, y por otro, y como novedad, se infringe el artículo 6 al suprimirse las imágenes suponiendo esto un tratamiento sin legitimación ya que la reclamante había solicitado las mismas para ejercer acciones en defensa de sus derechos. Prevalece en este caso la necesidad de mantener las imágenes frente a la obligación de supresión de estas.

También relacionado con la videovigilancia, cabe destacar la actuación de investigación **AI/00357/2022** por la que se archiva la reclamación presentada por la instalación de una cámara de videovigilancia, por el uso de las imágenes para sancionar al trabajador y por su entrega a la policía. Se informaba de la presencia de cámaras con carteles de videovigilancia y se instaló una nueva cámara perfectamente a la vista en el sistema ya instalado con motivo de los robos que se estaban produciendo, enfocando al lugar preciso

y durante el tiempo estrictamente necesario. Se considera que la instalación fue proporcional y estaba suficientemente informada.

El procedimiento sancionador **PS/00258/2022** tiene como distinción que permite que las cámaras de videovigilancia capten un espacio de vía pública ligeramente superior al espacio que venimos considerando de forma habitual como proporcional, debido a la naturaleza de los ataques vandálicos que sufre el inmueble del responsable y a su gravedad. Las cámaras no captan viviendas colindantes. Únicamente se impone una sanción por la infracción del art. 13 RGPD.

En el procedimiento de derechos **PD/00235/2022** contra Ferrocarriles de la Generalitat Valenciana, el reclamante formula el derecho de acceso solicitando, entre otras cuestiones, el acceso a dos grabaciones. Respecto de una de ellas el responsable del tratamiento dice que no se ha grabado y que no dispone de ella. Ahora bien, respecto de la segunda, el reclamado le ha dejado ver una transcripción, pero se niega a darle copia de la misma en atención a dos cuestiones que alega a lo largo del procedimiento: la confidencialidad y el secreto de la comunicación al tratarse de una infraestructura crítica y la afectación negativa a los derechos de terceros en virtud del art. 15.4 del RGPD. Por ello se discute en el procedimiento la atención incompleta del derecho de acceso.

Respecto de lo alegado por la parte reclamada, se contesta que no se ha encontrado limitación alguna al ejercicio de los derechos establecidos en los artículos 12 a 22 del RGPD en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Por otro lado, la parte reclamada no concreta ni ha evaluado cuál es la posible afectación negativa a los derechos de otro, tan sólo lo alega, resultando preciso conforme al artículo 15.4 del RGPD demostrar que el cumplimiento de la solicitud tiene efectos negativos sobre los derechos y libertades de otros participantes, los intereses de todos los participantes deben sopesarse teniendo en cuenta las circunstancias específicas del caso y, en particular, la probabilidad y gravedad de los riesgos presentes en la comunicación de los datos.

Asimismo, la parte reclamada afirma en sus alegaciones que si la Agencia le obliga a dar copia se limitará a la parte de la transcripción que afecta a la parte reclamante.

Se indica en la resolución estimatoria, que el reclamante tiene derecho de acceso a los datos personales que le conciernen, que comprenden todos aquellos que le conciernan y no sean exclusivos de terceras personas. Por tanto, no vale como excusa la salvaguarda del otro interlocutor ya que la transcripción de la conversación sería suficiente para proteger los datos personales del tercero. Además, en el supuesto examinado si se elimina de la transcripción la parte del otro interlocutor el derecho de acceso quedaría sin contenido. Máxime cuando la transcripción ya se ha mostrado al interesado.

No todos los procedimientos sancionadores acaban en sanción, un 11% de ellos se han resuelto con archivo. Este es el caso del **PS/00253/2021** contra el Club Deportivo San Roque en el que se reclamaba por parte de madres de niños de 7 años federados en la Federación de Futbol de Madrid la recepción de llamadas por parte del coordinador deportivo del Club, lo que supone la obtención de los teléfonos y los nombres de los niños. La parte reclamada alega que los teléfonos los obtuvo de un padre de otro de los jugadores y que los nombres de los jugadores figuran publicados en la página web de la Federación. Además, se invoca como base jurídica de la licitud del tratamiento efectuado, su interés legítimo en contactar con las madres para comunicarles la oferta de que sus hijos jueguen en el club la temporada siguiente. El procedimiento termina en un archivo de la infracción del art. 32 del RGPD, pero en apercibimiento por infracción del 5.1.f.

También se archivó el **PS/00413/2020**, contra Unísono Soluciones de Negocio SA. La empresa dispuso la modalidad de teletrabajo ante el estado de alarma. Para ello habilitó varias salas de videoconferencia y en una de ellas los trabajadores se podían ver a lo largo de toda la jornada laboral. Durante la instrucción del procedimiento se verifica la voluntariedad del uso de la cámara, sin condiciones ni consecuencias perjudiciales para el empleado.

Contra la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos se recibió una reclamación en nombre de numerosas personas por haber revelado datos personales a terceros a través del correo electrónico. Sin embargo, la Agencia no puede actuar como autoridad de supervisión en el supuesto objeto de análisis dada la inmunidad existente sobre Naciones Unidas y sus organismos especializados como se recoge en la Carta de Naciones Unidas en su artículo 105, en las Convenciones sobre Prerrogativas e Inmunidades de las Naciones Unidas y de sus Organismos especializados; y en otros tratados bilaterales y multilaterales.

El **PS/00386/2021** tiene su origen fuera de las fronteras españolas: fue un ciudadano alemán quien presentó la reclamación contra Amadeus IT Group SA al no haber obtenido respuesta adecuada en su solicitud de ejercicio de derechos (acceso y supresión). Ante la existencia de varias sucursales y direcciones de correo electrónico, el ciudadano alemán optó por escribir a la dirección de la filial alemana. El procedimiento finaliza con una sanción de 5.000€ por infracción del artículo 12 del RGPD en relación con el 15 (derecho de acceso).

Misma estructura tiene el **PS/00001/2022** contra Vacaciones eDreams SL, iniciado por una reclamación presentada ante la autoridad de control de Austria por falta de atención del derecho de supresión. Se dirige a la entidad un apercibimiento por la infracción del art. 12 del RGPD, en relación con art 17 del RGPD.

Finalmente, se han de destacar los procedimientos sancionadores iniciados contra responsables del sector público por incumplimiento de los requerimientos de esta Agencia, que se han detallado en el apartado 4 de la Agencia en cifras: Inspección de datos de esta Memoria.

Ante la falta de constancia del nombramiento de Delegado de Protección de Datos (DPD), se requirió a los ayuntamientos de Majadahonda, los Llanos De Aridane, Cambre, Arrecife, Aranda De Duero, Moncada, Algete, y San Andrés Del Rabanedo, para que procedieran a su cumplimiento. El nombramiento de DPD y su comunicación a la Agencia suponen obligaciones incluidas en el artículo 37 del RGPD para las autoridades u organismos públicos. Ante la falta de cumplimiento, se les sanciona por una infracción del art. 37 del RGPD, tipificada en el artículo 83.5.b), y calificada como grave a efectos de prescripción en el artículo 73 de la LOPDGDD.

Por otra parte, la Empresa Municipal Transportes Urbanos de Gijón, el Ayuntamiento de Monesterio, el Ayuntamiento de Oria, el Ayuntamiento de Burgos, la D.G. De La Guardia Civil y Establecimientos Residenciales para Ancianos de Asturias fueron todos ellos sancionados por la falta de acreditación de las medidas correctivas impuestas por resolución de la Directora, lo que supone una infracción del art. 58.2 del RGPD, tipificada en el artículo 83.6 y calificada como muy grave a efectos de prescripción en el artículo 72.1 de la LOPDGDD.

En virtud del art. 77.2 de la LOPDGDD, todos estos responsables públicos fueron sancionados con apercibimiento.

6. Una organización resiliente y en permanente mejora

6.1. Captación de talento y compromiso con el bienestar laboral

El RGPD, dispone en su artículo 52.4 que "cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité".

Tras más de dos años desde la entrada en vigor de la nueva normativa, el Parlamento Europeo el 25 de marzo de 2021 emitió un informe de evaluación de la Comisión acerca de la ejecución del RGPD señalando la importancia de que las autoridades de control de la Unión dispongan de suficientes recursos financieros, técnicos y humanos para poder hacer frente rápida, pero exhaustivamente a un número cada vez mayor de casos complejos y que requieren una gran cantidad de recursos, y para coordinar y facilitar la cooperación entre las autoridades nacionales de protección de datos, hacer seguimiento adecuadamente de la aplicación del RGPD y proteger los derechos y libertades fundamentales.

Es por ello que, a lo largo del año 2022 se ha realizado un importante esfuerzo para adaptar la relación de puestos de trabajo de la Entidad y mitigar, en cierto modo, el incremento en el volumen y en la complejidad de las labores realizadas en la AEPD.

Durante 2022 se procedió a la creación de catorce nuevos puestos, así como a la reclasificación de otros ocho puestos para fortalecer determinadas áreas de trabajo que han adquirido nuevas funciones y mayor relevancia, de manera que se garantice un funcionamiento adecuado de

aquellas, y al incremento del complemento específico de algunos puestos vinculado a un cambio significativo en el contenido funcional de los mismos que vieron incrementada su especial dificultad técnica, dedicación y responsabilidad.

Con el fin de garantizar la máxima cobertura de los puestos previstos en la RPT de funcionarios de la AEPD, a lo largo de 2022 se convocaron los procedimientos de provisión de puestos de trabajo siguientes:

- Concursos: tres concursos específicos y dos concursos generales, afectando a un total de 21 puestos de trabajo.
- Libres designaciones: seis convocatorias, afectando a un total de 25 puestos de trabajo.
- Publicaciones en Funciona de 14 puestos de trabajo.

Con todo ello, se alcanza un elevado grado de ocupación de los puestos de la entidad, debiendo destacarse la presencia femenina en los niveles predirectivos. Antes de la aprobación del Plan de Igualdad de la AEPD en 2020 partíamos de un 61,54 % de hombres frente a un 38,46 % de mujeres en dichos puestos. La cifra actual es del 42%, la cual se prevé aumentar en los tres años.

Sin embargo, el aumento en la entrada de documentación y la mayor dificultad que ésta presenta produce una tensión en la estructura y en los recursos que no se ha visto correspondida con un paralelo aumento del personal, de modo que muchas de las funciones de la Agencia se encuentran limitadas por la falta de capacidad para dedicar recursos a las investigaciones que se precisan.

Esa falta de dotación adecuada de efectivos ha llevado a una situación de estrés y de empleados exhaustos. Durante 2022 se llevaron a cabo dos mediciones de estrés: una inicial, para el conocimiento de la situación de ansiedad y el estrés percibido entre los trabajadores de la AEPD; y otra al final del año, una vez implantadas una serie de **medidas de bienestar emocional** (yoga, mindfulness y meditación). Las cifras obtenidas en la segunda medición del estrés indican que la ansiedad, el estrés percibido y la depresión han disminuido de manera estadísticamente significativa tras la realización de estas actividades. Por su parte, la salud física y la reevaluación cognitiva (regulación emocional) ha aumentado de forma significativa. Además, hay que señalar que la calidad de vida, la salud psicológica, las relaciones sociales y el buen ambiente de trabajo han aumentado con la realización de estas actividades. En efecto, la AEPD tiene el objetivo de favorecer el clima laboral y fomentar una óptima gestión del personal, está comprometida con el bienestar de su personal, demostrando que existe, y que funciona, una forma de liderazgo que tiene en cuenta el bienestar personal y laboral, la conciliación y la solidaridad.

Así mismo, en la tarea de captación de talento, el **teletrabajo** ha desempeñado un papel fundamental, dado el carácter pionero que la Agencia ha tenido en este régimen de trabajo con anterioridad incluso a la pandemia y que tan buenos resultados ha supuesto en la gestión. El objetivo es mejorar la calidad de la prestación de los servicios públicos a través de una organización más dinámica, susceptible de afrontar los retos de una organización del trabajo cada vez más flexible e incrementar la productividad y la conciliación del desarrollo profesional con la vida personal. En este marco de conciliación hay que referirse igualmente a otras acciones incardinadas en el Plan de Igualdad de la AGE como fue la visita al Museo del Prado de las personas trabajadoras con sus hijos/as menores en los primeros días de septiembre, antes del inicio del curso escolar.

Además, esta modalidad de trabajo se ha revelado como una medida que contribuye a cumplir los compromisos que con el medio ambiente aparecen recogidos en el **Plan de Responsabilidad Social de la AEPD** para el periodo 2019-2024, al reducir el número de desplazamientos in itinere, y con ello, las emisiones de gases de efecto invernadero, así como el consumo de electricidad en las dependencias de la Agencia.

Igualmente, no es posible entender el marco del teletrabajo en la AEPD sin tener en cuenta nuestro **código ético** que viene a blindar el compromiso del trabajador con su desempeño laboral con independencia de que se realice de forma presencial desde nuestra sede o de manera no presencial mediante teletrabajo. El código ético de la AEPD viene a suponer un marco de garantías que comprometen al trabajador en su desarrollo profesional mediante el establecimiento de obligaciones y responsabilidades del empleado público que viene a definir un alto grado de profesionalidad y exigencia de atendiendo a principios de igualdad, no discriminación, innovación, transparencia, confidencialidad, seguridad, conciliación laboral, sin perjuicio de nuestros compromisos con la sociedad.

Y destacar, igualmente, el compromiso de los empleados de la AEPD con la sociedad a través de actividades de voluntariado como charlas informativas impartidas por la Fundación ONCE sobre las diferentes opciones de participación en programas de atención a la diversidad o los donativos anuales que se realizan por el personal

de la AEPD durante la campaña de Navidad a una ONG elegida por la mayoría de los trabajadores entre varias propuestas. Este año 2022 las donaciones fueron destinadas a la Asociación Española contra el Cáncer, lográndose una contribución de más de 3.000 euros, superando la del año anterior.

6.2. Avance en digitalización

La AEPD destina gran parte de sus acciones a crear una Agencia más transparente, con una buena gestión organizacional que permita proceder siempre de la manera más ética e íntegra posible.

Para ello publica toda información organizativa, retributiva, económica y de publicidad activa exigida, primando la claridad, el orden y su accesibilidad, a través del sitio web sobre Transparencia que posee la Agencia. A este respecto, hay que destacar el Informe 2022 de revisión del cumplimiento de las recomendaciones efectuadas por el Consejo de Transparencia y Buen Gobierno (CTBG) en materia de Publicidad Activa por parte de la AEPD, en el que otorga una valoración del grado de cumplimiento de las obligaciones de publicidad activa del 95,2%, produciéndose un incremento de 17,5 puntos porcentuales respecto al año anterior. Así pues, el CTBG valoró muy positivamente la evolución del cumplimiento de las obligaciones de publicidad activa por parte de la AEPD y señaló que bastaría con que se publicase información sobre las modificaciones de contratos y el organigrama en formato reutilizable para que el nivel de cumplimiento se sitúe en el 100%, lo que se procedió a implantar en los primeros meses del 2022.

En el afán de mejorar la relación de ciudadanos y entidades con la Agencia a través de medios digitales, además de la sustitución de los números de atención telefónica por números de tarificación gratuita, la Secretaría General, a través de su departamento de tecnologías de la información ha seguido avanzando en iniciativas de digitalización y en la constante evolución de su infraestructura tecnológica, para disponer de los medios técnicos adecuados para el desempeño de su cometido,. Los hitos más destacados sobre los componentes y el contenido del portal web institucional han sido:

- Disponibilidad del canal de suscripción mediante fuentes RSS a nuevos tipos de contenido, para que cualquier persona pueda recibir un aviso cuando se publique una nueva resolución, un informe jurídico, una guía o una infografía.
- Incorporación de filtros facetados en los listados dinámicos de las guías, infografías, notas de prensa y entradas de blog para ofrecer al visitante una idea de las temáticas sobre las que hay contenidos etiquetados y el número de resultados que pueden consultar sobre cada una de ellas.
- Configuración del envío de campañas de correo electrónico y una sección en el portal institucional para lanzar el boletín mensual de noticias a las entidades adheridas al «Pacto Digital».
- Publicación de dos nuevas áreas temáticas, una con contenido específico de *salud y protección de datos* y otra con información sectorial dirigida a las *administraciones públicas*.
- Asistente *Asesora Brecha* para que un responsable pueda evaluar la obligación de notificar una brecha de datos personales a la Autoridad de Control y la nueva versión del asistente *Evalúa Riesgo*, sustituyendo la descarga de un fichero Excel por una aplicación web ejecutable en el navegador.
- Página promocional en el portal institucional para el lanzamiento de la campaña institucional *Más que un móvil* con UNICEF y la mejora del posicionamiento orgánico (o SEO) en buscadores para ayudar a su divulgación.
- Actualización del portal de menores *Tú decides en internet*, sustituyendo integralmente la plataforma de gestión de contenidos y diseñando una portada más moderna y cercana al público al que está dirigido.
- Mejora de la integración del gestor de contenidos con el gestor documental para poder publicar contenidos (principalmente, las resoluciones y los informes jurídicos anonimizados) con las etiquetas de un catálogo común (o tesauro) de conceptos y tipos de contenido relacionado con el que utilizan

las aplicaciones de tramitación, para poder utilizar una misma terminología entre todos los contenidos del portal, con independencia del sistema del que procedan.

En el ámbito de la administración electrónica, continúa la estrategia de adopción de los medios y servicios comunes, como la puesta en funcionamiento del componente eUTILS para el sellado electrónico y la evolución de la integración con los nuevos servicios del registro electrónico GEISER y del servicio de notificaciones NOTIFICA, para permitir a las aplicaciones de tramitación nuevas funcionalidades como, p.ej., dirigir una misma notificación a varios destinatarios (representante y titular) o poner a disposición notificaciones sólo en carpeta ciudadana y en la dirección electrónica habilitada única.

Además, se ha integrado la consulta automática de la representación al registro electrónico de apoderamientos en los formularios de la sede electrónica para incorporar el resultado de la consulta a las entradas que se trasladan a las unidades de tramitación y se han desarrollado los formularios de presentación de quejas y sugerencias de accesibilidad, de conformidad con el RD 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

En el ámbito de la tramitación electrónica de procedimientos administrativos, se ha avanzado en la digitalización de la gestión de las consultas previas al inicio del tratamiento del artículo 36 del RGPD y en la estabilización del sistema de gestión de la atención a consultas y a las comunicaciones de delegados de protección de datos.

En la tramitación de la gestión de reclamaciones se ha seguido mejorando la elaboración de documentos y el tratamiento de plantillas, se han incluido las adaptaciones para realizar la primera notificación a sujetos obligados a través del medio postal (en cumplimiento del artículo 43.2 del RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos) y la activación de la consulta a los datos del padrón desde la propia aplicación.

Así mismo, se ha habilitado el sellado y la firma electrónica de documentos en formato PADES y se ha evolucionado la integración con el servicio web de remisión de expedientes a Justicia (INSIDE), permitiendo ampliar los límites de formato, número y tamaño máximo de cada fichero.

Se ha continuado con la automatización de flujos de trabajo internos de la AEPD, como en el envío de comunicaciones en los acuerdos de inicio, las comunicaciones de traslado o los recordatorios de obligaciones en las admisiones a trámite; con las funciones de auditoría para la adecuada trazabilidad y seguimiento de los procesos ejecutados. Además, se ha definido y puesto en marcha un

plan de trabajo de dos años para seguir avanzando con la automatización y mejora de la aplicación de gestión de reclamaciones.

Se ha seguido colaborando en las iniciativas con el Ministerio de Justicia para la robotización y automatización de procesos, la utilización de técnicas de inteligencia artificial en la anonimización de documentos y la realización de actos de trámite en remoto , para las finalidades que se han descrito en otro apartado de la memoria.

Internamente, la Agencia ha continuado con actuaciones de modernización y actualización tecnológica de infraestructura de sistemas y aplicaciones, en la ubicuidad del puesto de trabajo y de los servicios disponibles en internet, y en los medios audiovisuales de la sede de Jorge Juan, ante la recuperación de los eventos presenciales y su retransmisión en directo por *streaming*.

Por último, se ha seguido trabajando en la adopción de prácticas y herramientas de gestión de servicios de tecnologías de la información, en la sistematización de indicadores y en el mantenimiento y securización del puesto de trabajo, una prioridad con entidad propia, por el contexto internacional y en la Administración General del Estado en particular, con el lanzamiento de los servicios del Centro de Operaciones de Ciberseguridad (CoCS).

6.3. Gestión eficiente de los recursos

Ejecución presupuestaria del presupuesto de gastos

Para el ejercicio 2022, el crédito inicial de gastos aprobado para la Agencia Española de Protección de Datos ha ascendido a 16.884.170 euros. Esto supone un incremento del 7,1% respecto al presupuesto de 2021. Se debe destacar que dicho incremento se ha concentrado en el Capítulo I, gastos de personal, donde se ha producido un incremento del 12,9% sobre el año 2021, tras las solicitudes al Ministerio de Hacienda para hacer frente a la grave carencia de personal antes descrita. Por contra, el total del crédito inicial de 2022 del resto de capítulos se ha reducido un 0,1% con respecto al crédito correspondiente a 2021.

Durante el ejercicio económico 2022 se han aprobado dos modificaciones presupuestarias internas al presupuesto del Capítulo I, gastos de personal, de la AEPD. Ambas transferencias tuvieron como objetivo incrementar el crédito presupuestario destinado a productividad y gratificaciones del personal, adecuando el importe del crédito inicial a los importes autorizados por la Secretaría de Estado de Presupuestos y Gastos, una vez certificados por la AEPD los valores de los indicadores definidos en el Modelo de Productividad Adicional por Cumplimiento de Objetivos, así como para la adecuación de dicho crédito inicial para el cumplimiento de Real Decreto-Ley 18/2022, de 18 de octubre y a las necesidades derivadas de la creación de nuevos puestos de trabajo. El crédito se transfirió desde otros conceptos del capítulo 1, cuya previsión de ejecución permitía considerar como presupuesto disponible parte de su importe inicial por lo que podía ser utilizado para atender las necesidades antes descritas.

El nivel de ejecución continúa situándose por encima del 90% en la línea de los últimos ejercicios presupuestarios y se ha situado en un 91,9% para el año 2022.

En relación con el grado de ejecución del Plan Estratégico de Subvenciones, se ha logrado un satisfactorio grado de ejecución presupuestaria, así como de los indicadores de actividad previstos en dicho Plan Estratégico de Subvenciones.

Asimismo, es de destacar que durante el ejercicio económico 2022 y siguiendo las recomendaciones de la Intervención Delegada, se han desarrollado diversas iniciativas de mejora en el área de la gestión del presupuesto de gastos tales como el desarrollo de procedimientos y manuales en el ámbito de la gestión de la tesorería y gestión del inventario que se implementarán a inicios de 2023.

Ejecución presupuestaria del presupuesto de ingresos

Como en años anteriores, el presupuesto aprobado para la Agencia para el ejercicio 2022 se financia mayoritariamente a través de unas previsiones de ingresos por recargos, sanciones e intereses de demora de 14.533.440 euros y, con un remanente de tesorería por un importe de 2.319.530 euros. El resto se cubre con las previsiones de transferencias corrientes (transferencias de la UE) por un importe de 20.000 euros, y con las previsiones de préstamos por un importe de 11.200 euros.

Durante el año 2022, el importe de los derechos reconocidos brutos asciende 20.831.686,06 euros, correspondiendo el 99,4% (20.711.341,49 €) a derechos reconocidos por las sanciones impuestas por resoluciones de la directora de la Agencia Española de Protección de Datos. Los derechos reconocidos netos ascienden a 20.397.178,32 euros, una vez contabilizadas las insolvencias o anulaciones producidas durante este año.

La recaudación total en el ejercicio corriente 2022 asciende a 18.631.260,83 euros, de los que 18.510.916,26 euros corresponden a sanciones (un 99,3%). La recaudación neta de sanciones, en el ejercicio corriente 2022, ha sido de 18.244.442,21 euros, una vez contabilizadas las devoluciones de sanciones.

Teniendo en cuenta que, junto con la recaudación del ejercicio, también se produce recaudación de derechos reconocidos de ejercicios cerrados durante el ejercicio corriente, la recaudación total de sanciones en el ejercicio de 2022 asciende a 34.426.290,16 euros, y la recaudación neta total de sanciones ha sido de 34.159.816,11 euros, una vez contabilizadas las devoluciones de ingresos como consecuencia de la estimación parcial o total de recursos. Esta recaudación, ha permitido la financiación de todo el presupuesto de gastos de la AEPD, sin necesidad de utilizar el remanente de tesorería.

La devolución de sanciones en el año 2022 asciende a 356.474,05 euros y el pago de intereses de demora como consecuencia de la estimación total o parcial de recursos potestativos de reposición o contencioso-administrativos ascendió a la cantidad de 16.496,05 euros.

En este ejercicio 2022, tras el cambio de política monetaria a nivel europeo, también se ha recaudado por el pago de los intereses de las cuentas corrientes abiertas en CAIXABANK y en el Banco de España a nombre de la AEPD que ha supuesto un ingreso en el ejercicio 2022 por importe de 108.632,91 € (capitulo 5 de ingresos). Del mismo modo, se ha vuelto a viajar a la Comisión Europea, lo que ha supuesto unos ingresos por reembolso de la UE por importe de 6.366,61 euros (capitulo 4). A este importe se añaden 3.882,70 euros de ingresos correspondientes a reintegros de préstamos concedidos al personal.

Durante el año 2020, por Orden de la Ministra de Hacienda y en cumplimiento del Real Decreto Ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, la AEPD tuvo que realizar un ingreso en el Tesoro Público de 21 millones de euros para contribuir a las necesidades económicas derivadas de la COVID-19, lo que supuso una merma de alrededor de un 40% del remanente de tesorería de la AEPD. No obstante, a lo largo del ejercicio 2022, dicho remanente, en la cuenta que la AEPD mantiene en el Banco de España, se ha incrementado por un total de 18,8 millones, habiéndose recuperado entre los años 2021 y 2022, la contribución realizada al Tesoro.

Presupuesto 2021 - 2022 Presupuesto, obligaciones reconocidas y porcentaje de ejecución

2022

Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	9.882.840,00 €	9.505.277,87 €	96,18%
Gastos corrientes en bienes y servicios	5.359.840,00 €	4.818.377,76 €	89,90%
Gastos financieros	350.950,00 €	160.954,37 €	45,86%
Transferencias corrientes	350.990,00 €	347.990,00 €	99,15%
Inversiones reales	928.350,00 €	669.939,18 €	72,16%
Activos financieros	11.200,00 €	6.629,14 €	59,19%
TOTAL	**16.884.170,00 €**	**15.509.168,32 €**	**91,86%**

2021

Descripción	Presupuesto	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	8.967.328,00 €	8.284.068,81 €	92,38%
Gastos corrientes en bienes y servicios	5.211.088,34 €	4.881.792,69 €	93,68%
Gastos financieros	350.950,00 €	124.655,41 €	35,52%
Transferencias corrientes	350.983,66 €	344.983,66 €	98,29%
Inversiones reales	861.350,00 €	828.773,06 €	96,22%
Activos financieros	20.800,00 €	0,00 €	0,00%
TOTAL	**15.762.500,00 €**	**14.464.273,63 €**	**91,76%**

DIFERENCIAS 2021 - 2022

Descripción	Presupuesto	Obligaciones reconocidas
Gastos de personal	915.752,00 €	1.221.209,06 €
Gastos corrientes en bienes y servicios	148.751,66 €	-63.414,93 €
Gastos financieros	0,00 €	36.298,96 €
Transferencias corrientes	6,34 €	3.006,34 €
Inversiones reales	67.000,00 €	-158.833,88 €
Activos financieros	-9.600,00 €	6.629,14 €
TOTAL	**1.121.670,00 €**	**1.044.894,69 €**

7. La necesaria cooperación institucional

7.1. Consejo Consultivo

El Consejo Consultivo, órgano colegiado de asesoramiento de la AEPD, se reúne cuando lo convoca la directora de la AEPD, que ostenta su presidencia, o cuando lo solicite la mayoría de sus miembros y, al menos, una vez cada seis meses.

En la práctica se reúne dos veces al año (normalmente en julio y en diciembre), aunque se mantiene contacto con sus miembros de forma bilateral en múltiples ocasiones.

En 2022, la secretaria del Consejo, por orden de la dirección, convocó 2 reuniones que se celebraron el 13 de julio y el 15 de diciembre de 2022, reuniones en las que se expuso y analizó la actividad del organismo.

En la reunión del 13 de julio destacó el análisis del fuerte incremento de actividad de la AEPD en todas sus subdirecciones y divisiones, las reestructuraciones internas para dar respuesta a ese incremento y las soluciones que se han encontrado para solventar esa gran carga de trabajo. Asimismo se incidió en las actividades de salud y bienestar emocional para los empleados de la Agencia, que se han valorado extraordinariamente.

En la reunión del 15 de diciembre, además de exponer la actividad de las distintas subdirecciones, se designaron los trabajos premiados en la convocatoria de los premios de la AEPD de 2022. En efecto, los miembros del Consejo son el jurado que resuelve los premios de Protección de Datos que se convocan anualmente y la resolución de los mismos es el principal asunto del orden del día de la reunión de diciembre.

Ambas reuniones se celebraron en formato mixto, aunando la presencialidad de algunos de sus miembros y facilitando la intervención telemática de los que no se desplazaron hasta nuestra sede, aprovechando las facilidades introducidas en la Ley 40/2015. de 1 de octubre, de Régimen Jurídico del Sector Público, que prevén la posibilidad de que las sesiones se celebren a distancia, las convocatorias se remitan por medios electrónicos y que se puedan grabar las sesiones.

7.2. Autoridades autonómicas

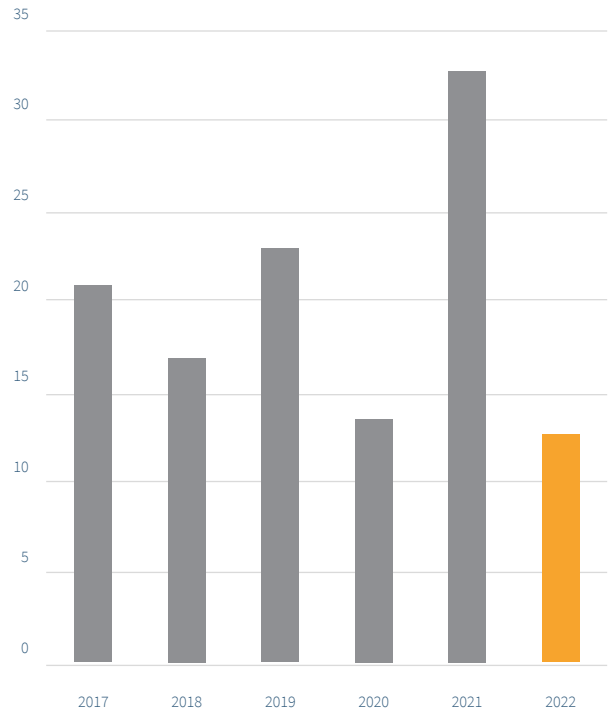
En el mes de mayo de 2022 se celebró una reunión con participación de la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía en las que se trataron temas relacionados con el proyecto Espacio de Datos de la Comisión de Sanidad Digital, la normativa aplicable a la videovigilancia policial, la participación de las CCAA en la actualización de la guía del Cloud de la AEPD , el Inventario de documentos elaborados por el Comité Europeo de Protección de Datos, el ejercicio del derecho de acceso establecido en el RGPD, el uso de firma biométrica y el alcance de la prohibición de ubicación fuera de la UE de sistemas de información para determinados tratamientos.

Asimismo, fueron convocadas en las reuniones del Consejo Consultivo de la Agencia Española de Protección de Datos con el fin de abordar las cuestiones, que se describen en otro apartado de la memoria.

7.3. Relaciones con el Defensor del Pueblo

Durante el presente año 2022 se han tramitado un total de 12 asuntos, frente a los 33 del pasado año.

Evolución quejas DP



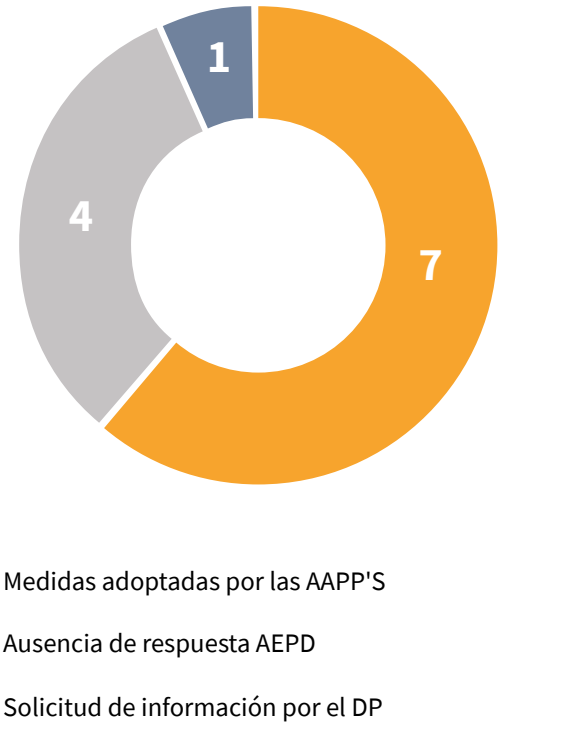
En cuanto a las materias o asuntos objeto de queja, el mayor número de ellas son solicitudes del propio Defensor del Pueblo requiriendo información sobre las medidas adoptadas por las administraciones públicas para el cumplimiento de las resoluciones de la Agencia.

Junto a ellas, destacan una solicitud de informe sobre las comunicaciones de datos por tres organismos del Ministerio del Interior a la Tesorería General de la Seguridad Social sobre las denegaciones de solicitudes de protección internacional.

Motivos de queja

Respecto a los motivos que han llevado a los ciudadanos a dirigirse a la AEPD mediante este cauce, el principal de ellos, en cuatro ocasiones, ha sido el relativo a la queja por la falta de respuesta en plazo de la resolución de las correspondientes reclamaciones o solicitudes de información formuladas ante la Agencia. De los restantes, junto a las ya mencionadas solicitudes de información sobre las medidas adoptadas por las administraciones públicas en cumplimiento de las resoluciones de la Agencia, así como las solicitudes de información sobre la tramitación de expedientes, destaca la antes citada sobre cesión de datos que dan lugar a la denegación de solicitudes de protección internacional.

Motivos de queja



8. Una autoridad activa en el panorama internacional

8.1. Unión Europea

8.1.1.Comité Europeo de Protección de Datos (CEPD)

La actividad del Comité Europeo de Protección de Datos ha sido intensa a lo largo del año 2022.

La Agencia Española ha participado de forma muy activa en estos trabajos. Por una parte, la Agencia está representada en todos los subgrupos de expertos del Comité Europeo. Por otra, actúa como coordinador de uno de sus subgrupos, el denominado su subgrupo de Cumplimiento, Salud y Gobierno Electrónico (Compliance, Health and eGovernment)

Finalmente, la Agencia ha participado como redactor principal o corredactor en varios de los documentos que el Comité ha publicado en 2022.

a) Directrices

A fin de cumplir con su misión de garantizar la aplicación coherente en toda la Unión Europea del RGPD, el CEPD ha continuado con su labor de elaboración y aprobación Directrices que clarifiquen y proporcionen orientación sobre distintos aspectos de la aplicación del Reglamento. Durante el año 2022 CEPD ha aprobado las siguientes Directrices:

i) Sobre Códigos de Conducta como instrumento de transferencias

El uso de los Códigos de Conducta (CdC) como instrumentos para proporcionar garantías adecuadas para la realización de una transferencia internacional está previsto en el artículo 46 RGPD y es una de las novedades que el Reglamento presenta.

La importancia de este nuevo instrumento de transferencias evidente, pues a través de su adhesión al mismo ofrece importantes ventajas tanto para los interesados como para los responsables y encargados del tratamiento.

Los responsables y encargados del tratamiento pueden utilizar la adhesión a estos códigos como prueba de que cumplen con la exigente normativa comunitaria, reforzando así su imagen pública tanto a nivel nacional como a nivel internacional comprometiéndose con la protección de datos en sus operaciones.

Sin embargo, precisamente la novedad del instrumento ha hecho necesario que el CEPD elabore estas directrices a fin de ofrecer guía sobre algunos aspectos esenciales de la configuración de los CdC a los fines de transferencias internacionales.

El plenario del Comité adoptó una primera versión para consulta pública en su reunión del mes de julio de 2021.

Tras la consulta pública, se recibieron numerosas contribuciones. El principal punto que se aborda en estas contribuciones es decidir si los CdC, como instrumento de transferencia internacional:

- Requieren tener siempre validez general dentro de la UE (art.40.5 y 40.9 del Reglamento).
- O si se trata de un instrumento de transferencia que no requiere necesariamente la exigencia de esa validez general dentro de la Unión y puede estar limitado a uno solo o varios estados miembros.

En debates posteriores se adoptó la primera opción, de conformidad con lo dispuesto en el art. 40.1 del Reglamento, argumentando que los

CdC como instrumento de transferencia requieren siempre, al igual que sucede con el régimen de las cláusulas tipo de protección de datos reguladas en el art.46.2 letras c y d del Reglamento, el cumplimiento de una doble condición: la aprobación por parte de la autoridad de control respectiva y la decisión de la Comisión Europea.

Finalmente, en el Plenario de febrero de 2022 se adoptaron esta Directrices 04/2021 en materia de Códigos de Conducta que pueden ser accedidas a través del enlace: *https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf*

ii) Sobre los derechos de los ciudadanos – el derecho de acceso

El Comité Europeo de Protección de Datos pretende elaborar una serie de directrices en torno a los derechos que el RGPD reconoce a los ciudadanos. Para ello se ha comenzado con estas estas directrices enfocadas al derecho de acceso.

Las directrices abordan aspectos tales como la no necesidad de justificación por parte del interesado a la hora de ejercer este derecho, al ámbito del derecho especialmente cuando afecta a derechos de terceros, la información adicional que debe contener la respuesta al derecho de acceso aparte de los propios datos personales del interesado, así como el formato y la vía por la que el responsable del tratamiento debe de facilitar el derecho con especial consideración cuando el volumen de información a proporcionar sea grande.

También se abordan en las directrices los casos en los que el responsable puede rechazar el ejercicio del derecho, así como aquellos casos en los que el responsable de tratamiento puede exigir el pago del coste de dicho ejercicio, teniendo en cuenta que, como regla general, el derecho debe ser gratuito.

Durante el 2022, esta directriz ha tenido una primera aprobación, a la que puede accederse a través del enlace: *Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu)* habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

iii) Sobre el mecanismo de cooperación del artículo 60 del RGPD

El objetivo de estas directrices es abordar la compleja casuística que surge en el proceso de colaboración entre la autoridad principal y las autoridades interesadas en los casos transfronterizos contemplados en el artículo 60 del RGPD.

Si bien ya el antiguo GT29 desarrolló una guía al efecto, posteriormente adoptada por el CEPD tras su constitución, dicha guía resultó claramente insuficiente tras su aplicación a los primeros casos transfronterizos.

La nueva directriz aborda los intercambios de información entre las autoridades implicadas desde el comienzo del caso hasta la presentación del primer borrador de decisión y comprende los artículos 60.1 y 60.3.

También se contempla la posibilidad (artículo 60.2) de que las autoridades implicadas en un caso transfronterizo puedan hacer uso de los mecanismos de asistencia mutua y operaciones conjuntas recogidos en el RGPD.

Se aborda también la interacción entre las autoridades implicadas tendentes a negociar una decisión final a partir de primer borrador de decisión y comprende los artículos 60.4 al 60.6.

Finalmente, se aborda la adopción y notificación de la decisión final a las partes involucradas en el caso y comprende los artículos 60.7 a 60.10, así como el procedimiento de urgencia descrito en el artículo 60.11

La AEPD ha formado parte del equipo de redacción de esta guía.

Se puede acceder a esta directriz a través del enlace: *Guidelines 02/2022 on the application of Article 60 GDPR | European Data Protection Board (europa.eu).*

iv) Sobre los patrones engañosos en las interfaces de las plataformas de las redes sociales: como reconocerlos y evitarlos

El objetivo de estas directrices es ofrecer recomendaciones prácticas a los diseñadores y usuarios de las plataformas de redes sociales sobre cómo evaluar y evitar los llamados "patrones engañosos" en las interfaces de las redes sociales que infringen los requisitos del RGPD.

El documento incluye una lista de patrones engañosos y mejores prácticas, así como los casos de uso, aunque esta lista no es exhaustiva. Los proveedores de redes sociales siguen siendo responsables de garantizar el cumplimiento del RGPD de sus plataformas.

La AEPD ha formado parte del equipo de redacción de esta guía.

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede accederse a través del *enlace*, habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

v) Sobre el cálculo de multas administrativas bajo el RGPD

El objetivo de estas directrices es proporcionar una serie de pautas a las autoridades de supervisión del RGPD para el cálculo del importe de las multas relativas a infracciones al RGPD, con el fin de armonizar dichos importes,

Estas directrices complementan unas directrices anteriores del Comité (sobre la aplicación y el establecimiento de multas administrativas en el Reglamento, WP253, respaldadas por el Plenario de 25 de mayo de 2018) y cuya aplicación práctica había puesto de manifiesto sus carencias.

Las nuevas directrices pretenden además de armonizar la metodología a seguir para el cálculo de los importes de las multas, pretende incrementar la claridad y transparencia en este tipo de operaciones, así como garantizar la aplicación y cumplimiento del Reglamento.

Este documento especifica lo dispuesto por el artículo 83 del Reglamento, que establece una serie de condiciones generales para la imposición de multas. Entre otras cosas, este artículo dispone que cada autoridad garantizará que las multas sean efectivas, proporcionadas y disuasorias. También establece una serie de criterios a tener en cuenta por las autoridades de control al decidir la imposición de multas y su cuantía en cada caso individual.

En cualquier caso, es necesario tener siempre en cuenta que las reglas generales que contienen estas directrices se entienden sin perjuicio de las circunstancias específicas y concretas de cada expediente.

La AEPD ha formado parte del equipo de redacción de esta guía.

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede accederse a través del *enlace*, habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

vi) Sobre reconocimiento facial en el ámbito de la cooperación policial

El objetivo de estas directrices es proporcionar una serie de pautas para alinear al RGPD los tratamientos de reconocimiento facial en el ámbito de la cooperación policial.

La guía señala que las autoridades policiales y judiciales usan cada vez más tecnologías de reconocimiento facial para identificar a personas a partir de fotografías o videos con diferentes finalidades y con el apoyo de otras tecnologías adicionales tales como la inteligencia artificial, el "machine learning" o el "big data".

Entre las finalidades, se encuentran el tratamiento de listas de sospechosos o la monitorización de los movimientos de las personas en espacios públicos. Estos tratamientos a gran escala pueden afectar a derechos fundamentales como el derecho a la privacidad y producir discriminación e incluso falsos resultados.

La guía establece que toda limitación al ejercicio de los derechos y libertades fundamentales debe contar con una base legal y respetar la esencia de esos derechos y libertades. El fundamento jurídico debe ser suficientemente claro en sus términos para dar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades están facultadas para recurrir a cualquier medida de recopilación de datos y vigilancia secreta, por lo que, a juicio del Comité Europeo de Protección de Datos, una mera transposición al derecho nacional de la cláusula general contenida en el artículo 10 de la Directiva (UE) 2016/680 (directiva LED) no sería válida al carecer de la precisión y previsibilidad necesaria en la limitación de los derechos y libertades fundamentales.

La guía apuesta por una prohibición del uso de estas tecnologías en espacios públicos y aboga por el respeto de los principios de finalidad y proporcionalidad de los tratamientos de datos en uso de estas. Además, las medidas legislativas destinadas a implantar su uso deben ser adecuadas para alcanzar los objetivos legítimos perseguidos por la legislación en cuestión. Un objetivo de interés general, por fundamental que sea, non puede en sí mismo, justificar una limitación a un derecho fundamental. Las medidas legislativas deben diferenciar e identificar a las personas que son objeto de ellas a la luz del objetivo concreto, por ejemplo, la lucha contra delitos graves específicos.

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede accederse a través del *enlace*, habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

vii) Sobre la puesta en práctica de soluciones amistosas

El objetivo de estas directrices es proporcionar una serie de pautas sobre que se entiendo y como se implanta un procedimiento soluciones amistosas a la hora tratar reclamaciones en el RGPD.

Hay que destacar que no todos los países cuentan en sus procedimientos administrativos nacionales con la posibilidad de gestionar reclamaciones al RGPD de forma amistosa, siendo España un ejemplo de ello, por lo que dichas directrices no son de aplicación a la gestión de reclamaciones que lleva a cabo la AEPD.

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede accederse a través del *enlace*.

viii) Sobre la Certificación como instrumento para las transferencias internacionales.

El RGPD exige en su artículo 46 que los exportadores de datos establezcan garantías adecuadas para las transferencias de datos personales a terceros países u organizaciones internacionales. A tal fin, el RGPD diversifica las garantías adecuadas que pueden utilizar los exportadores de datos en virtud del artículo 46 para enmarcar las transferencias a terceros países mediante la introducción, entre otras cosas, de la certificación como nuevo mecanismo de transferencia (artículo 42, apartados 2 y 2, letra f) del RGPD).

Estas directrices proporcionan orientaciones sobre la aplicación del artículo 46, apartado 2,

letra f), del RGPD sobre las transferencias de datos personales a terceros países o a organizaciones internacionales sobre la base de la certificación. El documento se estructura en cuatro secciones que abordan, entre otros, el proceso de certificación, la acreditación de los organismos de certificación, los criterios de valoración de la normativa del país importador, las obligaciones generales de los exportadores e importadores, las normas para las transferencias posteriores, los mecanismos de reparación y ejecución, las acciones para situaciones en las que la legislación y las prácticas nacionales impiden el cumplimiento de los compromisos asumidos como parte de la certificación y las solicitudes para el acceso a los datos por parte de las autoridades de terceros países, los compromisos vinculantes entre los responsables y encargados no sujetos al RGPD pero adheridos al certificado que establecen mediante contrato u otro instrumento vinculante para cumplir las salvaguardas apropiadas proporcionadas por el mecanismo de certificación.

Además de las citadas cuatro secciones, se incluye un anexo con ejemplos de medidas suplementarias en línea con las recogidas en el anexo II de las Recomendaciones 01/2020, sobre medidas que complementan las herramientas de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE).

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede accederse a través del *enlace*, habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

ix) Sobre la identificación de la autoridad de supervisión principal de un responsable o encargado

Las presentes directrices tienen por objeto clarificar el concepto de establecimiento principal en el contexto de responsables conjuntos teniendo en cuenta las Directrices 7/2022 del Comité Europeo de Protección de Datos.

Las directrices abordan los conceptos de tratamiento transfronterizo, se aportan criterios para realizar un test que permita dilucidar si dicho tratamiento "afecta sustancialmente", según la definición de tratamiento transfronterizo recogida en el artículo 4 del RGPD, a interesados en más de un Estado Miembro y se analiza el concepto de establecimiento principal.

A partir de los conceptos anteriores, se proporciona un procedimiento para identificar la autoridad de supervisión principal en diferentes escenarios: establecimiento principal distinto del emplazamiento de la central administrativa en el Espacio económico Europeo, grupo de empresas, responsables conjuntos, otros casos límites, etc., aportándose ejemplos en cada escenario para una mejor comprensión.

Durante el 2022, esta directriz ha tenido una primera aprobación a la que puede acceder a través del *enlace*, habiendo sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

x) Sobre notificaciones de brechas de seguridad

Debido a ciertas dudas sobre las notificaciones de brechas de seguridad, el CEPD decidió modificar las Directrices publicadas por el antiguo Grupo de Trabajo del Artículo 29. La modificación se limita al párrafo 73 y aclara que la mera presencia en algún país de la Unión Europea de un representante de un responsable que esté fuera de la Unión no significa que se pueda usar automáticamente el sistema de ventanilla única. En esos casos, las brechas de seguridad deberán notificarse a todas las autoridades de protección de datos afectadas.

El Comité aprovechó esta modificación para corregir algunas erratas y adaptar el texto al nuevo formato de las Directrices del CEPD. Las Directrices se aprobaron en octubre y están accesibles en el siguiente *enlace*.

xi) Sobre relaciones entre el Art. 3 y el Capítulo V RGPD

Estas directrices son una consecuencia de las adoptadas hace ahora dos años sobre ámbito territorial del RGPD.

En el proceso de elaboración de aquellas directrices, se planteó la duda sobre la consideración que debería darse a las comunicaciones de datos desde encargados situados en la UE y responsables no establecidos en ella cuando esas comunicaciones se producían en el marco de tratamientos de datos sometidos al RGPD en virtud de su artículo 3.2. Varias delegaciones sostenían que, en la medida en que los datos abandonan la UE existiría una transferencia internacional, mientras que, para otras, el hecho de que los datos no salieran del ámbito de protección del RGPD suponía que no podía hablarse de transferencia internacional.

Para abordar esta duda se decidió entonces elaborar unas directrices específicas, en concreto las Directrices 05/2021 sobre la aplicación del art.3 en relación con las disposiciones sobre transferencias internacionales reguladas en el Capítulo V del RGPD que fueron sometidas a consulta pública tras su primera aprobación en 2021.

Tras la consulta se introdujeron diversas modificaciones y se llegó a que el CEPD definiera que se entiende por "transferencia internacional de datos", dado que esta definición no está presente en el RGPD, y tampoco estaba en la anterior Directiva 95/46.

Para el Comité, existe una transferencia internacional cuando se dan los tres siguientes requisitos:

- El responsable o el encargado esté sujeto al Reglamento en función de un determinado tratamiento.
- El responsable o encargado (exportador) comunique mediante el envío o haga por cualquier otra forma que los datos personales, sujetos a este tratamiento, pueden quedar a disposición de cualquier otro responsable, responsable conjunto o encargado (importador).
- El importador se encuentre en un tercer país o en una Organización Internacional, independientemente que al importador le resulte o no de aplicación el Reglamento respecto a un determinado tratamiento de acuerdo con el art.3 del Reglamento.

Como puede observarse, en esta definición de transferencia se incluye ya la respuesta a la controversia sobre la aplicación o no del concepto para los tratamientos sujetos al RGPD en virtud del art. 3.2, ya que, según el tercero de los requisitos, el hecho de que el importador se encuentre en un tercer país determina la existencia de transferencia con independencia del régimen al que esté sujeto el tratamiento en que se enmarca.

Esta conclusión está en línea con un acuerdo preliminar que el plenario del Comité alcanzó cuando se otorgó el mandato para elaborar las directrices que ahora se han aprobado.

Hay algunos otros elementos también de interés en las directrices, como pueden ser:

- No se considera transferencia el caso en que un responsable en un tercer país recoge datos personales directamente de un interesado en la UE, dado que no hay "exportador"
- No se considera transferencia el caso en que un empleado de un responsable en la UE viaja a un país tercero por razones profesionales y accede a los datos contenidos en los registros del responsable, dado que no existiría un "importador" distinto del propio responsable para el que el empleado trabaja.

Está previsto que el nuevo texto de estas Directrices se ha adoptado en el Plenario del CEPD del mes de febrero de 2023.

b) Dictámenes

i) Dictamen conjunto CEPD-SEPD sobre la extensión del Reglamento del certificado Covid-19

Puesto que la emergencia sanitaria provocada por la pandemia mundial seguía en vigor fue necesario extender la vigencia del Reglamento del Certificado Covid-19. El CEPD y el SEPD señalaron que la Comisión Europea no había realizado el preceptivo análisis de impacto en la protección de datos, por lo que era imposible determinar la necesidad y proporcionalidad del reglamento. También sugería algunos cambios en los datos incluidos en el certificado.

Puede acceder a estos documentos a través del *enlace*.

ii) Dictamen conjunto CEPD-SEPD sobre la propuesta de Reglamento de la Ley de Datos (Data Act)

La Comisión Europea propuso un reglamento para establecer unas reglas armonizadas para el acceso justo y uso de los datos generados en la Unión Europea. Estos datos provienen de múltiples fuentes, como dispositivos conectados del internet de las cosas, asistentes virtuales o incluso dispositivos médicos o sanitarios.

La propuesta conjunta del CEPD y el SEPD incide en reforzar el control en los derechos de acceso, uso y compartición de los datos. También recomienda detallar los casos de "necesidad especial" para que las entidades públicas accedan a cualquier fuente de datos privada. Por último, se sugiere que las Autoridades de Protección de Datos tengan un papel activo en la vigilancia del cumplimiento de este reglamento.

Puede acceder a estos documentos a través del *enlace*.

iii) Dictamen conjunto CEPD-SEPD sobre la propuesta de Reglamento para establecer un Espacio de Datos de Salud Europeo (EHDS)

En el marco del denominado "estrategia de los datos", la Comisión Europea presentó una propuesta de reglamento para establecer un espacio de datos de salud europeo (EHDS). El objetivo es establecer un marco que permitir el acceso a los datos de salud de los ciudadanos europeos con todas las garantías necesarias para para facilitar asistencia sanitaria en situaciones de desplazamiento y para generar confianza con el fin de que estos datos se puedan reutilizar en investigaciones que redunden en beneficio de todos, así como generar una economía productiva de estos datos.

El CEPD y el SEPD sugieren varias modificaciones en la propuesta de reglamento para reforzar la capacidad de control de los europeos sobre el uso que se va a hacer de sus datos de salud, reforzando los principios y derechos establecidos en el RGPD. También recomiendan que se nombre a las Autoridades de Protección de Datos como las encargadas de vigilar el cumplimiento del Reglamento EHDS.

Puede acceder a estos documentos a través del *enlace*.

iv) Dictamen conjunto CEPD-SEPD sobre la propuesta de Reglamento para prevenir y combatir el abuso sexual infantil

Ante la necesidad de seguir protegiendo a los menores de edad de la explotación sexual de sus imágenes en internet, la Comisión presento una propuesta de reglamento que establece una agencia europea (Centro UE) encargada de identificar y perseguir el intercambio de este tipo de material audiovisual. El reglamento también obliga a los proveedores de servicios a establecer mecanismos que, en base a la información facilitada por el Centro UE, permita identificar y perseguir este tipo de materiales.

En su Dictamen, el CEPD y el SEPD señalan que algunos conceptos clave no están bien definidos, lo que podría afectar al juicio de necesidad y proporcionalidad de las medidas propuestas, en especial si conllevan el acceso de autoridades públicas. Avisan que el cifrado de los datos intercambiados es imprescindible para garantizar los derechos y libertades de los ciudadanos y obligar a descifrar los datos de los usuarios sería excesivo. El Reglamento concede un papel a las Autorida-

des de Protección de Datos en el mecanismo de supervisión. Sin embargo, la necesaria coordinación con el Centro UE puede resultar lesiva para la independencia de estas Autoridades.

Puede acceder a estos documentos a través del *enlace*.

v) Dictamen sobre los requisitos de acreditación de órganos de supervisión de códigos de conducta y entidades de certificación

El RGPD establece que los códigos de conducta deben contar con un órgano de supervisión que vigile el cumplimiento del código por parte de los responsables adheridos al mismo. Este órgano debe acreditarse por la autoridad nacional siguiendo unos requisitos de acreditación, que deben ser presentados al CEPD para su aprobación. Los requisitos aprobados durante 2022 mediante dictamen en aplicación del artículo 64 RGPD corresponden a los presentados por las autoridades de Eslovenia, Luxemburgo y Bulgaria,

De manera similar, antes de aprobar un mecanismo de certificación de acuerdo con el art. 42 del RGPD, es necesario establecer los requisitos de acreditación de las entidades de certificación que se dedicarán a emitir los certificados. Estos requisitos pueden ser elaborados por la propia autoridad o, si el organismo que se encarga de acreditar es el órgano de acreditación nacional (NAB), se deberán establecer requisitos adicionales a la norma ISO 17065. En cualquier caso, los requisitos deben aprobarse por el CEPD mediante dictamen. Durante 2022, las autoridades de Francia, Polonia y Bulgaria han recibido un dictamen favorable a sus requisitos de acreditación.

Puede acceder a estos documentos a través del *enlace*.

vi) Dictamen sobre esquemas de certificación

El RGPD prevé que algunos tratamientos puedan someterse a certificación para ayudar a demostrar que se realizan con seguridad y cumpliendo con el derecho fundamental a la protección de datos. Las entidades pueden elaborar esquemas de certificación que se someten al escrutinio y aprobación del CEPD.

Durante el año 2022 se aprobaron los esquemas de certificación denominados EuroPriSe y GDPR-CARPA. Por su parte, el esquema "Europrivacy" obtuvo el primer "Sello Europeo de Protección de Datos".

Puede acceder a estos documentos a través del *enlace*.

vii) Dictamen sobre Reglas Corporativas Vinculantes (BCR)

El RGPD prevé en su artículo 46.1 que, en ausencia de decisión de adecuación según el artículo 45.3 del RGPD, un responsable o encargado puede transferir datos personales a terceros países u organizaciones internacionales solo si el responsable o encargado del tratamiento hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Un grupo de empresas dedicadas a una actividad económica conjunta puede proporcionar tales garantías mediante el uso de BCR legalmente vinculantes, que confieren expresamente derechos exigibles a los interesados y cumplen una serie de requisitos (artículo 46 del RGPD). La implementación y adopción de BCR por parte de un grupo de empresas tiene como objetivo proporcionar garantías que se aplican de manera uniforme en todos los terceros países y, en consecuencia, independientemente del nivel de protección garantizado en cada tercer país.

Las BCR están sujetas a la aprobación de la autoridad de supervisión competente, de acuerdo con el mecanismo de consistencia establecido en el artículo 63 y 64.1 del RGPD que deben de comprobar que dichas BCR satisfacen las condiciones establecidas en el artículo 47, junto con los criterios establecidos por el CEPD en las directrices establecidas al efecto WP256 rev.01 del GT 29 y adoptadas por el CEPD)

Durante el año 2022 se aprobaron 23 BCR presentadas por varios países: Dinamarca, Eslovaquia, Francia, Alemania, Suecia, Liechtenstein, Irlanda, España y Hungría.

Estos documentos pueden ser accedidos en el *enlace*.

viii) Dictamen sobre la nueva propuesta de decisión de adecuación de los Estados Unidos de América

Como consecuencia del fallo del Tribunal de Justicia de la UE que declaraba la nulidad parcial del denominado "Escudo de Privacidad", el Comité Europeo de Protección de datos comenzó en 2022 los trabajos para una opinión sobre la nueva propuesta de acuerdo transatlántico entre la UE y los Estados Unidos que vendría a sustituir al Escudo de Privacidad. Se espera que la opinión del Comité Europeo de Protección de Datos sea presentada en el primer tercio del año 2023.

c) Recomendaciones

i) Recomendaciones sobre los elementos principales para tener en cuenta a la hora de aprobar las BCR-C

El 13 de noviembre de 2019, el CEPD encomendó al subgrupo de expertos de ITS ESG que trabajara en la elaboración de un documento público con el objetivo de clarificar los requisitos que han de reunir las BCR en relación con las obligaciones de los responsables y los encargados de BCR (BCR-C Y BCR-P) con el fin de garantizar unas mismas condiciones de igualdad para todos los solicitantes de BCR. El subgrupo de expertos ITS consideró que la forma más apropiada para dar cumplimiento al mandato era a través de las Recomendaciones previstas en el art.70.1.e del RGPD. Y comenzó a trabajar revisando los documentos públicos que se han publicado en estos últimos años en esta materia y procediendo a la actualización de los referenciales BCR-C y BCR-P ya existentes (recogidos en los documentos WP 256 rev.01 para BCR-C, y WP 257 rev.01 para BCR-P, y que habían sido aprobados por el CEPD). Asimismo, se decidió proceder a la fusión de los distintos referenciales con los formularios de solicitud normalizados que deben utilizar los solicitantes de las BCR (y que eran los correspondientes al WP264 del Grupo de Trabajo del Artículo 29 para BCR-C y al WP265 para BCR-P, respectivamente, y que también fueron aprobados por el CEPD).

Los miembros del ITS acordaron que sería más oportuno acometer, en primer lugar, el trabajo relativo al BCR de los responsables (BCR-C) con el fin de proporcionar a los solicitantes, lo antes posible, una guía actualizada sobre BCR-C, y trabajar después en la guía dirigida a los encargados (BCR-P). Y el ITS después de 3 años de trabajo ha conseguido finalizar un Borrador de Recomendaciones que contiene tanto los requisitos como el formulario normalizado de solicitud para BCR-C. y que se presentó al CEPD para su adopción en el Plenario de noviembre.

En cuanto al fondo, la modificación más importante que suponen estas recomendaciones en comparación con el «referencial» vigente, se refiere a la incorporación de los requisitos señalados por el TJUE en su Sentencia Schrems II. Esto se hace especialmente patente, en relación con los elementos principales contenidos en las nuevas Cláusulas Contractuales Tipo de la Comisión Europea para realizar transferencias internacionales de datos personales a terceros países.

Además, estas recomendaciones tienen como objetivo reflejar los resultados y los acuerdos alcanzados por las autoridades de protección de datos en el curso de los procedimientos de aprobación de solicitudes concretas de BCR desde la entrada en vigor del RGPD. La aprobación de las BCR es una tarea que deben desempeñar todas las Autoridades de Supervisión miembros del CEPD trabajando de la misma forma, y por ello es muy importante alcanzar un entendimiento común, entre todas las Autoridades de Supervisión, sobre los requisitos que deben incluirse en las BCR y en su formulario de solicitud.

Como resultado de la enseñanza de las mejores prácticas de las BCR en los últimos años, ha sido necesario ajustar la descripción de una serie de elementos que deben incluirse en las BCR con el fin de proporcionar una orientación lo más

precisa y al mismo tiempo lo más flexible posible a los solicitantes de BCR y facilitar el trabajo de las Autoridades de Control que ha de revisar las BCR s.

Estas Recomendaciones fueron adoptadas en el Plenario del CEPD de 14 de noviembre de 2022. Y fueron sometidas a consulta púbica el 17 de noviembre de 2022, cuyo plazo finalizará el 10 de enero de 2023.

Durante el 2022, estas recomendaciones han tenido una primera aprobación a la que puede accederse mediante el *enlace*, y que ha sido sometida a consulta pública, estando todavía pendiente la aprobación definitiva.

d) Decisiones vinculantes

A tenor del artículo 65 del Reglamento General de Protección de Datos, el Comité tiene potestad para adoptar decisiones vinculantes sobre cuestiones controvertidas, entre las autoridades líderes y las autoridades concernidas (con relación a los borradores de decisiones de las primeras relativas a tratamientos transfronterizos). Es el llamado mecanismo de resolución de disputas.

En el año 2022, el Comité ha adoptado las siguientes decisiones vinculantes:

i) Decisión vinculante del Comité 01/2022 (Accor)

El Plenario del Comité Europeo de Protección de Datos de 15 de junio adoptó su decisión vinculante 01/2022. La autoridad de control de Francia (CNIL) fue la autoridad líder en esta ocasión. En este expediente, el responsable fue el grupo hotelero francés ACCOR SA.

El caso se originó por unas quejas contra este grupo presentadas entre 2018 y 2020, relativas al envío de publicidad (sobre su grupo empresarial y sobre sociedades asociadas) y newsletters por parte de ACCOR, dentro de su programa de fidelización de clientes. Todo ello, pese a las solicitudes de baja de las personas que presentaron esas quejas.

El borrador de decisión de la CNIL estimó que ACCOR cometió infracciones a los artículos 12.1, 12.3, 13, 15.1, 21.2 y 32 del Reglamento General de Protección de Datos, y propuso una multa de 100.000 €. La autoridad de Polonia objetó el bajo montante de esta multa, que calificó de no efectiva, desproporcionada y no disuasoria.

En su decisión vinculante, el Comité estimó que la multa propuesta no era disuasoria. Por consiguiente, el Comité ordenó a la CNIL que la vuelva a calcular para cumplir los criterios del artículo 83.1 del citado Reglamento. La CNIL debía asegurarse de que esta sanción es proporcional y disuasoria, teniendo en cuenta la facturación del año precedente a la toma de la decisión.

A este documento se puede acceder mediante el *enlace*.

ii) Decisión vinculante del Comité 02/2022 (Instagram)

El Plenario del Comité de 28 de julio aprobó su decisión vinculante 02/2022. La autoridad de control de Irlanda (DPC) fue la autoridad de control líder en esta ocasión. META Platforms Ireland Limited (META) fue la responsable del tratamiento.

El caso concierne el tratamiento de datos relativo a menores (entre 13 y 17 años) realizado por META en INSTAGRAM (concretamente, la revelación al público de emails y teléfonos de estos a través de esa plataforma).

La decisión de DPC estimó que META cometió infracciones a los artículos 5.1, 12.1, 25 y 35 del Reglamento General de Protección de Datos. Teniendo en cuenta la naturaleza, duración y gravedad de estas infracciones, el hecho de que afectan a menores, así como el poder económico y los recursos globales del responsable, el Comité estimó que las multas deberían estar en la parte alta de las franjas fijadas por la decisión.

El Comité solicitó a DPC que vuelva a valorar la multa para garantizar que sea efectiva, proporcional y disuasoria. El Comité también estimó que

META IE cometió infracción adicional al artículo 6.1 del citado Reglamento, y que por tanto la autoridad de control de Irlanda también debe reflejar esta infracción en su decisión final.

A este documento se puede acceder mediante el *enlace*.

iii) Decisión vinculante del Comité 03/2022 (Facebook)

El Plenario del Comité de 5 de diciembre aprobó su decisión vinculante 03/2022, sobre FACEBOOK. La autoridad de Irlanda fue la autoridad líder en este caso. META Platforms Ireland Limited (META) fue la responsable del tratamiento.

En líneas generales, esta decisión versa sobre un borrador de decisión de Irlanda relativo a la legalidad y transparencia del tratamiento de publicidad dirigida (behavioral advertising).

Varias autoridades presentaron objeciones a este borrador, entre otras cosas, en torno a los principios generales de la protección de datos (artículo 5 del Reglamento General de Protección de Datos), la base legal para realizar tratamientos (artículo 6 del citado Reglamento) o las medidas correctivas a imponer (incluida la imposición de la multa).

En esta decisión vinculante, el Comité aclaró, entre otras cosas, la cuestión de si el tratamiento de datos para la ejecución de un contrato es una base legal apropiada en materia de publicidad dirigida.

A este documento se puede acceder mediante el *enlace*.

iv) Decisión vinculante del Comité 04/2022 (Instagram)

El Plenario del Comité de 5 de diciembre aprobó su decisión vinculante 04/2022, sobre INSTAGRAM. La autoridad de control de Irlanda fue la autoridad líder en este caso. META Platforms Ireland Limited (META) fue la responsable del tratamiento.

En líneas generales, esta decisión también versa sobre un borrador de decisión de Irlanda relativo a la legalidad y transparencia del tratamiento de publicidad dirigida (behavioral advertising).

Varias autoridades presentaron objeciones similares a este borrador, entre otras cosas, en torno a los principios generales de la protección de datos (artículo 5 del Reglamento General de Protección de Datos), la base legal para realizar tratamientos (artículo 6 del citado Reglamento) o las medidas correctivas a imponer (incluida la imposición de la multa).

En esta decisión vinculante, el Comité también aclaró, entre otras cosas, la cuestión de si el tratamiento de datos para la ejecución de un contrato es una base legal apropiada en materia de publicidad dirigida.

A este documento se puede acceder mediante el *enlace.*

v) Decisión vinculante del Comité 05/2022 (Whatsapp)

El Plenario del Comité de 5 de diciembre aprobó su decisión vinculante 04/2022, sobre WHATSAPP. La autoridad de Irlanda fue la autoridad líder en este caso. META Platforms Ireland Limited (META) fue la responsable del tratamiento.

En líneas generales, esta decisión versa sobre un borrador de decisión de Irlanda relativo a la legalidad del tratamiento con la finalidad de mejorar los servicios de esta plataforma.

Varias autoridades presentaron objeciones a este borrador, entre otras cosas en torno a los principios generales de la protección de datos (artículo 5 del Reglamento General de Protección de Datos), la base legal para realizar tratamientos (artículo 6 del citado Reglamento) o las medidas correctivas a imponer (incluida la imposición de la multa).

En esta decisión vinculante, el Comité aclaró, entre otras cosas, la cuestión de si el tratamiento de datos para la ejecución de un contrato es una

base legal apropiada por lo que respecta a los tratamientos para la mejora de servicios.

A este documento se puede acceder mediante el *enlace*.

e) Informes

i) Utilización de la nube (cloud) por el sector público

En el ejercicio de 2022 el Comité Europeo de Protección de Datos llevó a cabo su primera iniciativa dentro del Marco de Supervisión Coordinado (CEF, por sus siglas en inglés) que tuvo dentro del marco de A tenor del artículo 65 del Reglamento General de Protección de Datos, el Comité tiene potestad para adoptar decisiones vinculantes sobre cuestiones controvertidas, entre las autoridades líderes y las autoridades concernidas (con relación a los borradores de decisiones de las primeras relativas a tratamientos transfronterizos). Es el llamado mecanismo de resolución de disputas.

En su reunión del 17 de enero de 2023, el Plenario del Comité Europeo de Protección de Datos adoptó un informe sobre la utilización de servicios basados en la nube por el sector público ("Use of cloud-based services by the public sector").

Este documento se ha ido preparando previamente a nivel técnico a lo largo de todo el año 2022, dentro de la iniciativa llamada "Coordinated Enforcement Framework" (CEF). CEF ha presentado este documento con la finalidad de reforzar la protección de datos personales en este terreno.

El informe tiene en cuenta como referencia una serie de informes nacionales elaborados previamente por las autoridades de supervisión del Espacio Económico Europeo que voluntariamente decidieron participar y a las que se añadió el Supervisor Europeo de protección de datos cuyas potestades de circunscriben a los tratamientos realizados por las instituciones europeas.

Entre otras cosas, el informe del Comité presenta un resumen ejecutivo, describe esta iniciativa, muestra una serie de estadísticas sobre el tipo de actores contactados, detalla acciones de inspección acometidas por las autoridades de control y presenta recomendaciones para los organismos públicos.

La AEPD recuerda que los organismos públicos deben contratar servicios en la nube que cumplan totalmente con el Reglamento General de Protección de Datos. Es consciente de las dificultades que están encontrando los organismos públicos a la hora de realizar estas contrataciones, por lo que espera que gracias a esta iniciativa se consiga mayor efectividad y uniformidad en el cumplimiento a nivel europeo. Asimismo, también destaca la importancia de seguir las recomendaciones para los organismos públicos que presenta este informe.

A este documento se puede acceder mediante el *enlace*.

Los informes nacionales que han servido como base para la realización del informe europeo anterior pueden ser accedido en el *enlace*.

f) Declaraciones

i) Declaración sobre cooperación en materia de aplicación de la ley (declaración de Viena)

El Comité Europeo de Protección de Datos publicó una declaración en Viena el 28 de abril sobre cooperación de las autoridades de control en materia de cumplimiento del Reglamento General de Protección de Datos ("Statement on Enforcement Cooperation").

Dicha declaración presenta dos líneas de actuación:

1) Armonización de aspectos procedimentales:

Tiene como objetivo que el Comité identifique una lista de aspectos procedimentales que se podrían armonizar para maximizar el impacto del citado Reglamento. Para cumplir con este mandato, el Plenario de ese Comité de 10 de octubre decidió enviar una carta de su presidenta al Comisario de Justicia de la Comisión Europea.

En líneas generales, esta carta señala que el Comité considera prioritario armonizar procedimientos y que confía en que la Comisión apoye una serie de aspectos procedimentales armonizables. Se trata de solventar las disparidades existentes entre los diferentes procedimientos nacionales de los 27 estados miembros de la UE, así como de Islandia, Noruega y Liechtenstein.

Con este fin, el Comité ha presentado a la Comisión una lista de aspectos procedimentales para su posible armonización si el marco legal lo permite.

A partir de ahora la Comisión, que ha integrado esta iniciativa en su Programa de Trabajo, va a continuar trabajando en esta iniciativa con esta finalidad

2) Casos estratégicos

Las autoridades de Países Bajos, Bélgica, Alemania, Francia y España son 'rapporteurs' en esta iniciativa.

El Plenario del citado Comité adoptó el 12 de julio un documento que define los criterios a tener en cuenta para seleccionar estos expedientes. Para adquirir la condición de estratégico, estos casos deben reunir al menos uno de los siguientes criterios: Plantear un problema estructural o reiterativo en varios Estados miembros, relacionar la protección de datos con otros campos jurídicos, afectar a una gran cantidad de interesados en varios Estados miembros, abarcar un gran número de quejas en varios Estados miembros, derivar de un asunto o cuestión fundamental de la Estrategia 2021-2023 del Comité, o presentar un alto riesgo (según una serie de parámetros).

Esta enumeración no tiene carácter exhaustivo. Estos casos serán en principio y prioritariamente del mecanismo de ventanilla única del Reglamento General de Protección de Datos (el llamado "One-Stop-Shop").

Ese mismo Plenario también adoptó un segundo documento que traza el proceso a seguir para estos expedientes. Las autoridades de control son quienes proponen casos, que en última instancia no pueden seleccionarse sin el consentimiento y aceptación de las autoridades que los lideran. Cada expediente debe tener asociado un pequeño grupo de entre 3 ó 4 autoridades de control, que en principio incluirá a la autoridad líder. No tienen por qué abarcar a todas las autoridades interesadas. La participación de estas es voluntaria

A este documento se puede acceder mediante el *enlace*.

ii) Declaración del Comité Europeo de Protección de Datos sobre las implicaciones de la Sentencia del Tribunal de Justicia de la UE en relación con los registros de nombres de los pasajeros de vuelos aéreo

El 21 de junio de 2022, por remisión del Tribunal Constitucional belga, el Tribunal de Justicia de la UE dictó sentencia sobre la Directiva del Registro de nombres de pasajeros de vuelos. Si bien el Tribunal consideró que la validez de la Directiva PNR no se ve afectada, dictaminó que, para garantizar el cumplimiento de la Carta de los Derechos Fundamentales de la UE, la Directiva PNR debe interpretarse en el sentido de que incluye importantes limitaciones al tratamiento de datos personales Algunas de estas limitaciones son la aplicación del sistema PNR únicamente a los delitos de terrorismo y delitos graves, que tengan un vínculo objetivo con el transporte aéreo de pasajeros, y la aplicación no indiscriminada del período general de retención de cinco años a todos los datos personales de los pasajeros.

La interpretación que propone el Tribunal reduce significativamente las formas en que los Estados miembros de la UE pueden tratar los datos PNR. El Comité Europeo de Protección de Datos considera probable que el tratamiento actual de los datos PNR en muchos, si no en la mayoría de los Estados miembros, no cumpla plenamente con la Directiva PNR tal como la interpreta el TJUE. Por lo tanto, los sistemas PNR en toda la UE pueden seguir interfiriendo de manera desproporcionada con los derechos fundamentales de los interesados todos los días. En su declaración, el EDPB pide a los Estados miembros de la UE que tomen todas las medidas necesarias a nivel legislativo y/o administrativo para garantizar que su respectiva transposición nacional e implementación de la

Directiva PNR estén en línea con la Carta tal como la interpreta el TJUE. En este sentido, el EDPB señala que las autoridades de protección de datos son plenamente competentes para investigar el cumplimiento de los requisitos de protección de datos de la UE a nivel nacional.

A este documento se puede acceder mediante el *enlace*.

8.2. Supervisión de los Sistemas IT de Cooperación Policial y Judicial del Espacio de Libertad, Seguridad y Justicia–nuevo Comité de Supervisión Coordinada

8.2.1.Comité de Supervisión Coordinada (CSC).

El Comité de Supervisión Coordinada deberá sustituir a las actuales autoridades comunes de supervisión de los sistemas informáticos en el ámbito de la Cooperación policial y judicial de la Unión Europea: SIS II (sistema Schengen), VIS (visados), Eurodac (inmigración), JSA y JIS (aduanas), Europol (policía europea) y Eurojust (órgano de cooperación judicial europea). Son objeto también de la supervisión coordinada las actividades de la Oficina de la Fiscalía Europea y del IMI (sistema informático de Mercado Interior. Por este motivo, las referencias a las autoridades comunes de los sistemas IT de Europol y Eurojust que ya han pasado a la nueva supervisión coordinada bajo el CSC se eliminan en esta memoria anual 2002.

El nuevo comité ha aprobado su programa de trabajo para el periodo 2022-2024, que desarrolla las actividades a realizar en el marco de la supervisión de los sistemas informáticos citados.

Este programa de trabajo ha seleccionado los derechos de los interesados como un área clave de actividad. El CSC reforzará la concienciación y proporcionará más orientación para ayudar a las personas a navegar por la red de sistemas y responsables de los tratamientos de los datos personales y la gran cantidad de reglas diferentes a la hora de ejercer sus derechos, también en vista de los desafíos que traerá el nuevo marco legal de interoperabilidad de los sistemas IT de la Unión Europea.

El Comité también se compromete a mejorar su diálogo con las partes interesadas, en particular con las ONG, academia e investigadores que trabajan en este campo, al promover la reflexión y el debate sobre temas de interés común. La transparencia es un principio rector de nuestro trabajo y el CSC utilizará su sitio web de manera más intensa, dentro del Comité Europeo de Protección de Datos (EDPB), para comunicarse con el público e informar sobre sus actividades.

8.2.2.Grupo de Coordinación de la Supervisión SIS II

La Agencia ha continuado desarrollando las actividades programadas en el marco de su Plan Actuación quinquenal de la Evaluación Schengen y participó además en la coordinación de la

evaluación Schengen de España llevada a cabo entre el 20 y el 25 de marzo de 2022 por parte del equipo auditor conjunto de la Comisión Europea y las Agencias nacionales de protección de datos.

Como continuación a la visita, y en cumplimiento del plan da actuación Schengen, la Agencia ha asistido a las reuniones convocadas por la Dirección General de Coordinación de Políticas Comunes y Asuntos Generales de la UE del Ministerio de Asuntos Exteriores con el fin de continuar con la coordinación de las actuaciones de cara a la ejecución del plan de evaluación continua del derecho a la protección de los datos personales en el marco Schengen.

8.2.3.Grupo de Coordinación de la Supervisión VIS (SCG)

La Agencia coordinó la evaluación Schengen de España llevada a cabo entre el 20 y el 25 de marzo de 2022 que incluyó la auditoria del sistema VIS de visados.

El Grupo de coordinación aprobó el plan de actuación 2022-24 durante la primera reunión anual de 2022. A lo largo de este año se ha llevado a cabo el inicio de las acciones establecidas en el plan de actuación a lo largo del año 2022. Entre las actuaciones que se están ejecutando cabe señalar en primer lugar el seguimiento de la actualización del sistema VIS en ejecución del Reglamento (UE) 2021/1134, que tiene por objeto adaptar la política común de visados a nuevos retos, incluidos mayores riesgos de seguridad, nuevos patrones de migración irregular, altos riesgos epidémicos, necesidad de actualizaciones tecnológicas e interoperabilidad de los sistemas de información, y amplía el ámbito de aplicación del VIS para incluir información sobre visados para estancias de larga duración y permisos de residencia (así como sobre actualizaciones en materia de protección de datos),

Se incluye también entre las actuaciones el seguimiento de la ejecución del Reglamento (UE) 2021/1133, que establece cómo deben aplicarse la interoperabilidad y las condiciones para la consulta de los datos almacenados en los sistemas SIS (área Schengen), Eurodac (inmigración) y ECRIS-TCN (antecedentes penales de nacionales de terceros Estados), así como de los datos de Europol (policía europea) por el proceso automatizado del VIS a efectos de la identificación de respuestas positivas. De conformidad con su artículo 6, el presente Reglamento «se aplicará a partir de la fecha de inicio de la explotación del VIS de conformidad con el artículo 11 del Reglamento (UE) 2021/1134» que prevé que «a más tardar el 31 de diciembre de 2023, la Comisión adoptará una decisión mediante un acto de ejecución que fije la fecha en que comiencen las operaciones del VIS de conformidad con el presente Reglamento».

El VIS SCG podría llevar a cabo otras actividades para garantizar una transición fluida al nuevo conjunto de normas, especialmente a la luz de las recomendaciones formuladas por Supervisor Europeo de Protección de Datos en su dictamen 9/2018.

A partir de los debates en curso en el marco del VIS SCG, es posible enumerar las siguientes cuestiones para la evaluación del Grupo:

- Inspecciones coordinadas en los consulados (posible sinergia con el SIS II SCG);
- Transferencia de datos a terceros países u organizaciones internacionales (artículo 31);
- Auto-@ monitoreo: recogida y puesta en común de las mejores prácticas de las autoridades nacionales (artículo 35);
- Recomendaciones de evaluación de Schengen;
- Acceso a los datos para su verificación en el territorio de los Estados miembros (artículo 19);
- Acceso a los datos para el examen de la solicitud de asilo (artículo 22).

8.2.4.Grupo de Coordinación de la Supervisión de Eurodac (sistema de información huellas dactilares)

En su primera reunión anual del Grupo de Coordinación de la Supervisión del sistema IT de Eurodac (sistema informático del ámbito de inmigración) se aprobó el programa de actividades 2022-24.

Además de las actividades previstas, el GCS de Eurodac trabajará de forma permanente en el seguimiento de la evolución política y legislativa, cualquier cuestión en curso, el intercambio de experiencias y la asistencia mutua.

Otra de las actividades del GCS es el seguimiento de la propuesta de la Comisión Europea por la que se modifica la refundición de 2016 del Reglamento Eurodac.

La propuesta de la Comisión Europea de mayo de 2016 de refundir el Reglamento Eurodac tenía por objeto ampliar los objetivos del sistema Eurodac, facilitar los retornos y ayudar a abordar la migración irregular. La propuesta introdujo los siguientes cambios en el Reglamento Eurodac, que tienen importantes repercusiones en la protección de datos:

- Almacenar y consultar datos de nacionales de terceros países o apátridas que no sean solicitantes de protección internacional y que se encuentren en situación irregular en la UE para identificarlos con fines de retorno y readmisión;
- Almacenar más datos alfanuméricos, por ejemplo, nombres, fechas de nacimiento, nacionalidades, datos de identidad o documentos de viaje, así como imágenes faciales en Eurodac para permitir a las autoridades de inmigración y asilo identificar a los nacionales de terceros países sin tener que solicitar la información a otro Estado miembro por separado, como ocurre actualmente;
- Introducir sanciones de conformidad con la legislación nacional para las personas que se nieguen a cumplir el procedimiento de toma de impresiones dactilares.

8.3. Participación de la AEPD en otros foros internacionales

8.3.1.Comité Consultivo y Mesa de la Convención 108+ del Consejo de Europa

Durante 2022 la Agencia Española de Protección de Datos participó en las reuniones ordinarias del Comité Consultivo en formación de Plenario y Mesa. En 2022 se produjo la renovación de la mesa, órgano de dirección de los trabajos del Comité Consultivo. La Agencia forma parte de la mesa al haber sido elegido uno de los miembros de la delegación española como miembro de la misma.
Dado que la elección de los miembros es realizada a título personal la Agencia cuenta ahora con dos miembros en el comité con representación por lo tanto en ambos, Plenario y Mesa.

Como se mencionó en el informe de 2021, el Estado español ratificó en fecha 28 de enero de 2021 Convenio 108+ que ha sido depositado. Hasta finales de 2022, un total de 43 Estados han firmado la convención, de los cuales 14 han procedido también a su ratificación.

A continuación, se recogen los documentos aprobados por el Consejo de Europa en materia de protección de los datos personales durante el ejercicio 2021-22:

- **i) Guía sobre la identidad nacional digital**

Muchos países han adoptado esquemas de identidad nacional que procesan una variedad de datos personales incluyendo categorías especiales de datos sobre personas físicas para, principalmente, certificar la autenticidad de la "identidad legal" de un individuo ante la ley y frente al Estado.

Históricamente, los esquemas de identidad nacional comenzaron como sistemas de identidad "análogos" que se basaban en los datos limitados registrados en los sistemas de registro civil (nacimiento, matrimonio, defunción). Tales esquemas de identidad se basaron y aún pueden basarse en la emisión de una identificación fundacional 'documento' (como una tarjeta de identidad) por el cual una persona puede probar su identidad ante el derecho y frente al Estado, y por el que se puede conceder a los particulares el acceso a los servicios públicos (como las protecciones de bienestar social) o mediante el cual podrían hacer valer sus derechos.

Cada vez más, los esquemas de identidad nacional analógicos se están digitalizando para incluir el tratamiento de datos personales a menudo acompañado de autenticación a través de datos biométricos como huellas dactilares y escáneres de iris. Estos esquemas de identidad nacional digitalizados también pueden incorporar un enlace a datos e identificadores demográficos y biométricos recopilados en otros sectores específicos sistemas tales como atención médica, bienestar social o incluso registro de tarjeta SIM móvil o móvil bases de datos de identidad de dispositivos. Los esquemas nacionales de identidad digital buscan representar el estatus legal de un individuo y puede afectar e influenciar muchos aspectos de la vida privada de una persona, incluyendo el ámbito privado de sus actividades digitales. Por ejemplo, se puede utilizar una identidad digital nacional en el sector comercial, para proporcionar servicios de aseguramiento de identidad.

Las directrices establecen un conjunto de medidas de referencia que los responsables de formular políticas y otras partes interesadas pueden aplicar a los esquemas de identidad, para ayudar a garantizar que dichos esquemas no socaven, sino que examinen adecuadamente, considerar y mitigar sus posibles impactos adversos sobre los derechos humanos y las libertades consagradas en los instrumentos internacionales pertinentes. Se pretende que las directrices ayuden a garantizar que el número de identidad digital nacional respete y proteja los derechos humanos y las libertades fundamentales, desde la fase de política a través de la fase de diseño y todos los aspectos del tratamiento de datos.

A este documento se puede acceder mediante el *enlace*.

ii) El spyware Pegasus y su impacto en los derechos humanos

El informe se hace eco del escándalo producido en numerosos Estados, muchos de ellos miembros del Consejo de Europa, como consecuencia del uso del spyware denominado “Pegasus” por parte de las fuerzas del orden con fines de interceptación y vigilancia de las comunicaciones de personas, tanto de personas públicas como de ciudadanos ordinarios, con fines de lucha contra el terrorismo y otras amenazas a la seguridad nacional.

La preocupación por garantizar la seguridad nacional y luchar contra las actividades delictivas puede justificar el uso excepcional de tecnologías de vigilancia de las comunicaciones. Los servicios policiales y de inteligencia han de verse legitimados para obtener la información necesaria, incluso mediante escuchas telefónicas y análisis de metadatos o de forma encubierta directamente desde dispositivos móviles para prevenir, investigar y enjuiciar delitos o combatir amenazas relacionadas con la seguridad nacional. Si bien, los Estados están obligados por normas internacionales, regionales e instrumentos nacionales de derechos humanos, como el Convenio Europeo de Derechos Humanos (CEDH) y la jurisprudencia pertinente de la Unión Europea y el Tribunal Europeo de Derechos Humanos. Los Estados miembros del Consejo de Europa tienen obligaciones negativas, es decir, abstenerse de interferencia con los derechos fundamentales y obligaciones positivas para proteger activamente estos derechos. Esto incluye también la protección de las personas contra la acción de actores no estatales.

El informe concluye que las consecuencias de la vigilancia masiva sobre personas mediante herramientas como Pegasus puede ser catastrófica en relación con los derechos y libertades funda-

mentales y servir a regímenes autoritarios para perseguir a los opositores y suprimir las libertades de expresión y de información. Por ello, el diseño, desarrollo e implantación de dichos sistemas y tecnologías debe venir acompañado de garantías efectivas que aseguren la protección de las personas y el equilibro entre los derechos y las libertades y los intereses en juego.

A este documento se puede acceder mediante el *enlace*.

b) Comité de Inteligencia Artificial

El Comité de Inteligencia Artificial representa a los 46 Estados parte del Consejo de Europa que son miembros del Comité y a cinco Estados que tienen la condición de observadores. Tiene como misión elaborar un texto consolidado de borrador de la primera convención del Consejo de Europa en materia de inteligencia artificial que será presentado a la aprobación de la Asamblea de Ministros del Consejo de Europa. La Convención tiene plazo de presentación a la asamblea hasta noviembre de 2023.

Hasta la fecha se han celebrado cuatro reuniones para la discusión del denominado "texto cero" de la convención que fue preparado por un comité ad hoc específico para la inteligencia artificial o CAHAI. La Comisión Europea lidera las negociaciones en colaboración con las delegaciones de los Estados parte del convenio.

8.3.2.Asamblea Global de Privacidad (GPA).

La Asamblea Global de Privacidad (GPA por sus siglas en inglés), que agrupa a la mayoría de las autoridades de protección de datos a nivel global, celebró en octubre de 2022 en Estambul su 44 conferencia anual organizada por la autoridad Mexicana INAI y la autoridad Turka de protección de datos (KVKK).

En la conferencia se aprobaron las siguientes resoluciones:

a) Resolución para modificar la hoja de ruta para lograr la Secretaría financiada en la práctica (2022-2026).

En la 40 Conferencia de 2018 se encomendó al Grupo de Trabajo sobre el Futuro de la Conferencia (FOTC) que preparara, en estrecha colaboración con el Comité Ejecutivo, una hoja de ruta para establecer una Secretaría financiada.

En la 43 Conferencia se aprobaron las modificaciones al reglamento de la nueva Secretaría, así como el modelo de estructura de cuotas y el calendario de implantación. Se aprobó también la disolución del FOTC y la creación de un Comité de Selección de la Secretaría que desarrollará las nuevas modalidades de recaudación de cuotas y recomendará una candidatura para sede de la Secretaría.

Debido a circunstancias imprevistas, el Comité de Selección de la Secretaría no ha podido desarrollar sus trabajos en los plazos previstos por lo que se ha hecho necesario ampliar el plazo inicial establecido en doce meses adicionales.

A este documento se puede acceder mediante el *enlace*.

b) Proyecto de Resolución sobre la creación de capacidades de cooperación internacional para mejorar la regulación de la Ciberseguridad y sobre la comprensión de los daños causados por los ciberincidentes (v1.9 final)

La creciente prevalencia de los ciberataques en todas las regiones del mundo exige una respuesta normativa sólida y coordinada para proteger los datos personales de las personas. Los actores gubernamentales y los grupos criminales ajenos al Estado suponen amenazas en el ciberespacio cada vez con más facilidad, en parte debido a la rápida aceleración de la interconexión digital de la sociedad desde el advenimiento de la pandemia por COVID-19, pero también debido a las vulnerabilidades de la cadena de suministro en los productos finales.

Desde el GPA se pretende contribuir a la mitigación y reparación de los ciberataques. Los miembros de

la GPA han llevado a cabo un importante volumen de investigaciones sobre incidentes cibernéticos en los que se ha descubierto un pésimo manejo de las categorías de datos más sensibles, como el cambio de sexo, los datos sanitarios y la identidad física (que podría incluir la raza o el origen étnico, etc.). La falta de concienciación en materia de seguridad en las organizaciones, la falta de responsabilidad en materia de seguridad de la información, la gestión eficaz de los riesgos y las comprobaciones periódicas a lo largo de la cadena de suministro suelen ser temas problemáticos.

Por lo anterior, el GPA ha resuelto adoptar las siguientes líneas de actuación:

- Adoptar medidas para desarrollar una comprensión de las competencias y responsabilidades de las autoridades miembros del PAM en relación con la ciberseguridad;
- Explorar las posibilidades de cooperación internacional, el intercambio de conocimientos e información, incluyendo la experiencia técnica y las mejores prácticas, entre los miembros de la GPA para evitar la duplicación en las investigaciones u otras actividades reguladoras en relación con los problemas de ciberseguridad y los enfoques reguladores en lo que respecta a la protección de datos y la privacidad;
- Solicitar al Grupo de Trabajo de Cooperación para el Cumplimiento de la Normativa Internacional de la GPA que realice un trabajo exploratorio para el otoño de 2023, teniendo en cuenta el trabajo realizado por otros Grupos de Trabajo de la GPA cuando sea pertinente y consultando con el Panel de Referencia de la GPA, según corresponda. La GPA también deberá determinar si prosigue el trabajo en el marco de su próximo Plan Estratégico a partir de 2023.
- Solicitar al Grupo de Trabajo de Cooperación Internacional para el Cumplimiento de la Normativa que acuerde un plan de trabajo para llevar a cabo los pasos anteriores, centrado en resultados claros y prácticos que deberían incluir la celebración de una sesión cerrada sobre cuestiones de ciberseguridad en 2023.

A este documento se puede acceder mediante el *enlace*.

c) Resolución sobre los Principios y expectativas para el uso adecuado de la información personal en la Tecnología de Reconocimiento Facial

La resolución pretende aportar directrices a las organizaciones que utilizan el reconocimiento facial basadas en una serie de principios:

- Fundamento legal: Las organizaciones que utilizan el reconocimiento facial deben tener un fundamento legal claro para la recopilación y el uso de datos biométricos.
- Proporcionalidad: razonabilidad, necesidad y proporcionalidad: Las organizaciones deben establecer, y ser capaces de demostrar, la razonabilidad, necesidad y proporcionalidad de su uso de la tecnología de reconocimiento facial.
- Protección de los derechos humanos: Las organizaciones deben, en particular, evaluar y proteger contra la interferencia ilegal o arbitraria de la privacidad y otros derechos humanos.
- Transparencia: El uso del reconocimiento facial debe ser transparente para las personas y grupos afectados.
- Rendición de cuentas: El uso del reconocimiento facial debe incluir mecanismos claros y eficaces de rendición de cuentas.
- Principios de protección de datos: El uso del reconocimiento facial debe respetar todos los principios de protección de datos, incluidos los mencionados anteriormente.

A este documento se puede acceder mediante el *enlace*.

9. La cooperación con Iberoamérica

En febrero la AEPD presentó como Secretaría Permanente de la RIPD un proyecto a la AECID para solicitar la financiación de distintas actividades, atendiendo a la convocatoria realizada dentro del programa Interconecta en diciembre de 2021.

El proyecto presentado fue aprobado y se incluían actividades de formación, webinarios, foro y asistencia en la organización de los Encuentros de la RIPD, estando previsto realizar todas estas actividades hasta entrado el año 2024.
Durante 2022, se han realizado tres Convocatorias del Consejo Consultivo, febrero, junio y julio, concretamente el de febrero dio como resultado la programación para el 31 de marzo de la presentación del estudio de capacidades instituciones de las autoridades de control en Iberoamérica, acto que finalmente se desarrolló. También se aprobó el plan de trabajo a realizar por la RIPD durante el año 2022.

En junio se aprobó la solicitud de observador presentada por la Subsecretaría de Políticas Públicas Basadas en Evidencia, dependiente de la Secretaría Innovación y Transformación Digital perteneciente a la Jefatura de Gabinete de Ministros del Gobierno de La Ciudad Autónoma de Buenos Aires.

En el marco de la conferencia sobre Computación, Privacidad y Protección de Datos 2022 (en inglés CPDP 2022) que ha tenido lugar en Bruselas entre el 23 y el 25 de mayo, se ha desarrollado un panel denominado "Convergencia en acción: cooperación regional y global entre autoridades de protección de datos". El panel organizado por la Comisión Europea ha tenido como panelistas a D. Waldemar Gonçalves Ortunho Junior Director Presidente de la Autoridad Nacional de Protección de Datos de Brasil, a Dª. Tamar Kaldani, vicepresidenta del Comité Consultivo del Consejo de Europa de la Convención 108 y exdirectora de la autoridad de protección de datos de Georgia, Dª. Drudeisha Madhub, Presidente de la Autoridad de Protección de Datos de Islas Mauricio y a D. Joaquín Pérez Catalán, Director de la División de Relaciones Internacionales de la AEPD.

En el debate se ha planteado entorno a la cooperación entre autoridades de protección de datos y como la normativa y las diferentes redes de autoridades han contribuido a fomentar dicha cooperación, así como la convergencia de actuaciones entre autoridades.

Por parte del Presidente de la Autoridad de Brasil así como del representante de la AEPD, en su calidad de Secretaría Permanente de la RIPD, se ha resaltado el importante papel realizado por la Red Iberoamericana de Protección de Datos (RIPD) a la hora fomentar la cooperación entre las autoridades de protección de datos del área. Como ejemplos de dicha cooperación se ha señalado la elaboración de los Estándares Iberoamericanos de Protección de Datos y las recientes Cláusulas Contractuales para Transferencias Internacionales de Datos.

El Foro de la Sociedad Civil, Observadores de la RIPD, han avanzado en su consolidación, disponen de una página web que les da visibilidad y donde han comenzado a publicar los estudios y documentos en relación con los derechos y libertades de las personas.

Se han mantenido reuniones con responsables de autoridades responsables en temas de privacidad como la autoridad argentina a la que se presentó la iniciativa del Canal Prioritario impulsado por la AEPD y se intercambiaron conocimientos y experiencias.

En septiembre, se celebró la reunión entre las autoridades AEPD como Secretaria Permanente y la Agencia de Protección de Datos de los Habitantes de Costa Rica, representada por su Directora. En dicha reunión se abordaron temas relaciones con la situación de la autoridad de Costa Rica, tales como presupuestos, procedimientos implantados, legislación actual o convenio 108 entre

otros. La AEPD ofreció a la autoridad de Costa Rica, el paquete de herramientas de que dispone actualmente y que puedan servir de utilidad para apoyar el desarrollo y avance de dicha autoridad.

En septiembre se mantuvo una reunión con el Foro de la Sociedad Civil para analizar su progreso, destacando como tema principal de la reunión el trabajo de investigación que están llevando a cabo sobre el estado actual de las autoridades en Iberoamérica a partir de información recabada de las páginas web de las autoridades.

En octubre en reunión con representantes de la Superintendencia de Colombia se puso de manifiesto que desde marzo no está designado ni el Superintendente de Comercio ni el Superintendente Delegado, dado el tiempo transcurrido señalaron que esperaban que el nombramiento se realizara en un corto plazo de tiempo. En la reunión, los representantes colombianos informaron de que estaban desarrollando una guía sobre BCR que compartirían con el resto de la RIPD en un corto plazo de tiempo.

También se mantuvo una reunión con representantes de Bolivia para analizar el estado del anteproyecto de Ley de Protección de Datos de Bolivia y posible calendario de aprobación, temas relacionados con el Convenio 108 o 108+ y sobre el modelo de autoridad de control prevista.

En este mismo mes se mantuvieron reuniones con representantes de la Unión Europea para valorar colaboraciones en la región.

Posteriormente, en noviembre se mantuvo una reunión con representantes de la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación donde se informó sobre los avances en la propuesta del anteproyecto de Ley de Protección de Datos de Bolivia.

Otras reuniones que destacar fueron las mantenidas con la Asociación Iberoamericana de Protección de Datos y Ciberseguridad donde se valoró la importancia de realizar actividades conjuntamente como webinarios relacionados con la gestión documental, protección de datos y ciberseguridad, programas de capacitación en distintos entornos como Educación, Instituciones Públicas o Pymes. Otro tema de interés estuvo relacionado con la atención a las víctimas de violencia digital.

Durante el ejercicio se ha actualizado también la web de la RIPD incluyendo el listado de guías y herramientas que cada país ha elaborado y que está disponible en su página web.

Por parte de la Secretaría de la RIPD se ha maquetado la guía de cláusulas contractuales que se encuentra ya disponible en la web.

Colombia ha comenzado a redactar una guía sobre BCR.

En marzo se realizó el primer taller de intercambio del Grupo de Trabajo de la RIPD para las relaciones con la industria de internet. El objetivo del taller fue que todas y todos los participantes puedan, proponer y escuchar las propuestas de temáticas que se deberían abordar, problemas identificados o líneas de acción generales a impulsar. Cada participante presentó y propuso temáticas generales que podrían abordar en un plan de trabajo futuro.

LA AGENCIA EN CIFRAS

1. Inspección de datos

1. El inicio de la potestad de supervisión. Reclamaciones, comunicaciones y actuaciones por iniciativa propia

La Subdirección General de Inspección de Datos (SGID, en adelante), es el órgano dependiente de la Directora de la Agencia, que, en caso de posible vulneración de la normativa, o de no atención al ejercicio de derechos, analiza los indicios, realiza las actuaciones de tutela o las de investigación oportunas, y cuando procede, instruye los procedimientos sancionadores para proponer a la Directora la adopción de la resolución que corresponda.

Las reclamaciones pueden recibirse directamente a la Agencia, que es la situación más frecuente, aunque también pueden llegar a través de alguna Autoridad de Control de alguno de los Estados miembros del Espacio Económico Europeo (EEE). Estas últimas tienen un carácter transfronterizo y se admiten a través del mecanismo de ventanilla única, establecido en el artículo 60 del RGPD; son reclamaciones presentadas en otro Estado miembro del EEE o trabajos en los que la Autoridad de Control (AC) del EEE ha decidido iniciar una actuación por propia iniciativa y la AEPD se encuentra afectada. Por ello, la SGID también evalúa su participación en la iniciación de procedimientos de cooperación de casos transfronterizos en los que otras AC nos comunican una presunta infracción.

Bien como consecuencia de las reclamaciones, bien por propia iniciativa, la Directora de la Agencia puede determinar la apertura de actuaciones de investigación para alcanzar una mejor y más concreta determinación de las conductas o hechos que puedan infringir la normativa de protección de datos. Durante el año 2022 ha bajado el número de investigaciones que se han realizado por propia iniciativa, debido a la falta de recursos para atender el volumen de trabajo creciente.

Dentro de los casos en los que se actúa por iniciativa propia hay que destacar las actuaciones de investigación que se realizan, cuando procede, a raíz de las notificaciones de brechas de datos personales. Las notificaciones se efectúan de acuerdo con el artículo 33 del RGPD. Estas brechas se reciben en primera instancia en la División de Innovación Tecnológica (DIT) de la AEPD y, tras un primer análisis, cuando existan datos objetivos que justifiquen un análisis en mayor profundidad, la Directora acuerda iniciar una investigación de oficio e instar a la Subdirección General de Inspección de Datos para que realice comience las previas de investigación tendentes a acreditar los hechos.

La siguiente tabla muestra estos datos y su comparación con los del ejercicio anterior:

Tabla 1: Entradas de nuevos casos a inspección					
Tipo de entrada	**2020**	**2021**	**2022**	**% relativo de 2022**	**Δ% desde 2020**
Reclamaciones* presentadas ante la AEPD	10.324	13.905	15.128	96%	46,5%
Casos transfronterizos procedentes de otras AC del EEE	784	581	651	4%	-17%
Propia iniciativa de la AEPD	107	85	43	0%	-59,8%
TOTAL	**11.215**	**14.571**	**15.822**	**100%**	**41,1%**

** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales le conciernan.*

Se puede observar que persiste la tendencia fuertemente creciente, con un aumento del 9% respecto al año 2021 y un 47% respecto del año 2020. Por segundo año consecutivo, el número de reclamaciones recibidas ante esta Agencia ha sido el mayor en la historia de la AEPD.

Además, se puede observar un incremento de un 12% en las reclamaciones transfronterizas que consumen más tiempo y esfuerzos debido a la necesidad de consenso con otras autoridades.

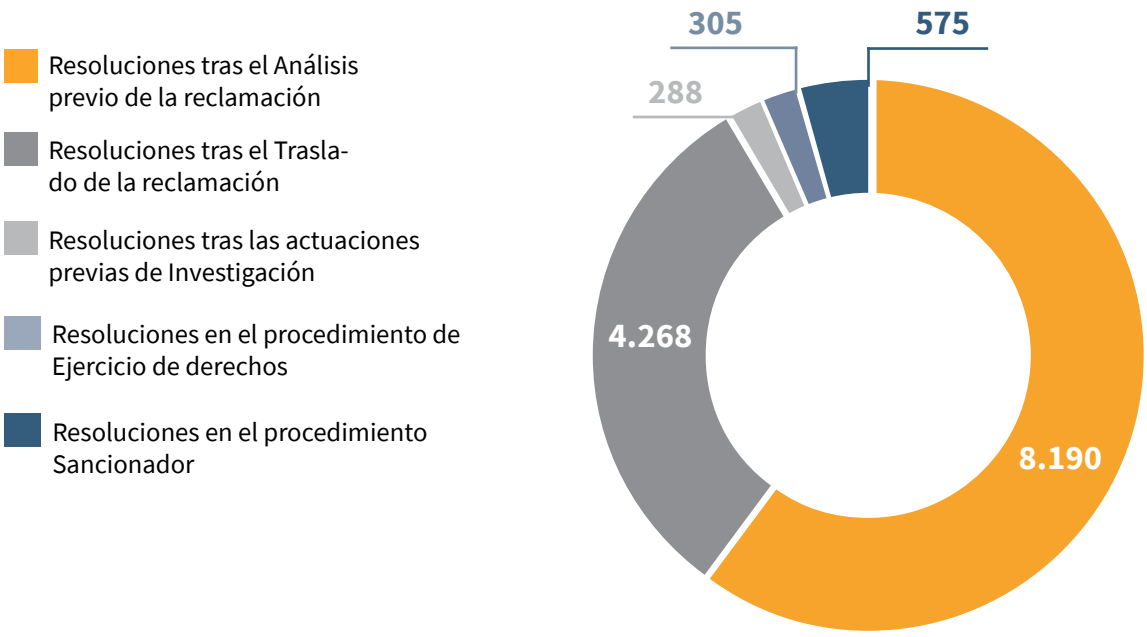
En 2022 la tasa de reclamaciones resueltas frente a reclamaciones recibidas se ha mantenido en el entorno del 100%, lo que pone en valor el compromiso de la Agencia con la resolución de las reclamaciones en este contexto de persistente aumento de la entrada. El número de reclamaciones resueltas ha sido también extraordinario en la historia de la Agencia, y un 6% superior al año anterior. En el Anexo B se analiza con más detalle cómo se correlacionan las mejoras de productividad con la implantación del teletrabajo en la Agencia. En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

Tabla 2: Reclamaciones resueltas y pendientes				
Tasa de resolución de reclamaciones	**2020**	**2021**	**2022**	**Δ% anual**
Reclamaciones* resueltas en el año	10.443	14.098	14.937	43%
Reclamaciones pendientes de resolver al finalizar el año	3.709	3.516	3.707	-0,1%
Tasa de reclamaciones resueltas vs. recibidas en el año	101%	101%	99%	-2%

** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales le conciernan.*

2. Resoluciones

Fase de resolución de las reclamaciones



Uno de los indicadores que muestran la actividad que se realiza desde la Subdirección General de Inspección de Datos es el número de resoluciones que se emiten. Las entradas reflejadas en el apartado anterior pueden dar lugar a diferentes actuaciones y procedimientos que finalizan en resoluciones. El número de entradas tramitadas no tiene que coincidir necesariamente con el número de resoluciones firmadas: varias reclamaciones referidas a una misma infracción y sujeto reclamado pueden agruparse y, paralelamente, en una reclamación pueden aparecer múltiples reclamados, dando origen a múltiples procedimientos y, por lo tanto, a diferentes resoluciones.

2.1 Resoluciones durante el Análisis previo de la Reclamación

La primera fase que se lleva a cabo en la tramitación de las reclamaciones es el análisis inicial de cada una de ellas. Comprende su clasificación, la verificación formal de su contenido y el análisis de competencia y de otras causas que afectan a su fundamento y admisibilidad. Es lo que se denomina la fase de análisis previo de admisibilidad de la reclamación.

Si del análisis se desprende que la reclamación no cumple los requisitos de admisibilidad establecidos en la normativa, se inadmitirá y, en caso contrario, prosperará a la siguiente fase. El motivo principal de inadmisión es el de no apreciarse indicios racionales de la existencia de una infracción en el ámbito competencial de la Agencia. El porcentaje de inadmisiones en esta fase se encuentra en el 60% de los casos, como muestra la siguiente tabla:

Tabla 3: Resoluciones en fase de Análisis previo de la reclamación				
Tipo de resultado	**2021**	**2022**	**% relativo**	**Δ% anual**
Resoluciones tras la fase de Análisis de la reclamación	**8.058**	**8.190**	**60%**	**2%**
Inadmisiones a trámite*	7.854	7.928	58%	1%
Competencia de otras AC nacionales (CGPJ, AC auton.)*	204	262	2%	28%
Resoluciones en otras fases	**5.053**	**5.436**	**40%**	**8%**
TOTAL	**13.111**	**13.626**	**100%**	**4%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

2.2 Resoluciones posteriores

Con la entrada en vigor del RGPD y, fundamentalmente, de la LOPDGDD, se introdujo una fase de traslado de la reclamación al responsable o encargado del tratamiento o, en su caso, al DPD, con la pretensión de resolver con mayor rapidez las reclamaciones, de acuerdo con las disposiciones del artículo 65 de la LOPDGDD. Estos traslados pueden conducir a la solución de la reclamación, o a aportar información que contribuya a clarificar la situación de manera que se pueda determinar que no ha existido infracción de la normativa de protección de datos. De esta forma, se consigue resolver un número elevado de reclamaciones en un tiempo reducido, con independencia de la actuación inspectora que siempre se puede realizar de acuerdo con las competencias que tiene atribuidas la SGID.

La inclusión de la fase de traslado ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. En 2022, tras haber procedido al traslado de la reclamación, se dictó resolución finalizando su tramitación en el 79% de los casos, dando así una respuesta más rápida a los reclamantes que la que se conseguía con la normativa anterior y solucionado de una manera más ágil su reclamación. Por su parte, la Agencia consideró la existencia de responsabilidades que debían ser depuradas en procedimiento sancionador en el 11% de los casos.

En la siguiente tabla se muestra la distribución completa de resoluciones según la fase en que se alcanza la finalización del caso.

Tabla 4: Resoluciones en fases posteriores				
Tipo de resultado	**2021**	**2022**	**% relativo**	**Δ% anual**
Resoluciones tras el Traslado de la reclamación* **	**3.679**	**4.268**	**79%**	**16%**
Respuesta satisfactoria del responsable o enc.	2.421	2.912	54%	20%
Ser plena competencia de otra AC del EEE	361	411	8%	14%
Actuar como autoridad interesada en el EEE (archivo provisional)	304	196	4%	-36%
Otros motivos tras traslado	593	749	14%	26%
Resoluciones tras las actuaciones previas de Investigación	**438**	**288**	**5%**	**-34%**
Archivo de actuaciones previas de investigación	438	288	5%	-34%
Resoluciones en el procedimiento de ejercicio de derechos	**351**	**305**	**6%**	**-13%**
Resuelto en el procedimiento de ejercicio de derechos	351	305	6%	-13%
Resoluciones tras procedimiento Sancionador	**585**	**575**	**11%**	**-2%**
Resuelto en procedimiento sancionador -Multa***	264	385	7%	46%
Resuelto en procedimiento sancionador - Apercibimiento	222	126	2%	-43%
Resuelto en procedimiento sancionador - Archivo	99	64	1%	-35%
TOTAL	**5.053**	**5.436**	**100%**	**8%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** El fundamento de estas resoluciones se describe en las filas siguientes.*

**** El detalle de las multas se describe en el apartado 8.*

Se observa una reducción de las resoluciones que se realizan como consecuencia de las actuaciones previas de investigación de la reclamación. Esto se debe a que las investigaciones terminan en un mayor porcentaje más elevado en procedimientos sancionadores, lo que refleja una mayor eficacia en el trabajo de la subdirección, ya que, hay menos actuaciones previas de investigación que terminen en un archivo.

2.3 Tiempos medios de resolución

Se reflejan a continuación los tiempos medios, en días, hasta que se dicta resolución. Debe tenerse en cuenta que las resoluciones que se realizan antes de la admisión a trámite son de inadmisión. Esto ocurre durante la evaluación de la reclamación, es decir, después del análisis previo y también después del traslado de la reclamación al responsable o encargado.

En fase de Análisis previo de la reclamación, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se resuelve su inadmisión, después de analizar la verificación formal del contenido y su fundamento. Debe tenerse en cuenta que el artículo 65.5 de la LOPDGDD establece un plazo de 3 meses para este concepto.

Tabla 5: Tiempo medio de resolución en análisis previo

Tiempos medios de resolución en fase de Análisis (en días)	2021	2022	Δ% anual
Resoluciones tras el Análisis de la reclamación*	26	25	-4%
TIEMPO MEDIO	**26**	**25**	**-4%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

Como se puede observar, este dato de 25 días es muy inferior al de los tres meses.

En la fase de traslado de la reclamación al responsable o encargado, el tiempo medio responde al tiempo desde que tiene entrada la reclamación hasta que se firma la resolución de inadmisión, tras el traslado al responsable y el análisis de la respuesta recibida. Nuevamente se puede observar que el tiempo medio es inferior a los tres meses y que se ha producido una reducción respecto de los tiempos del año anterior.

Pasadas estas dos fases, la reclamación se admite a trámite y se inician los procedimientos establecidos en la Ley. Los tiempos de resolución en actuaciones previas de investigación, en procedimientos de ejercicio de derechos y en procedimientos sancionadores, se contabilizan desde la fecha de admisión a trámite de la reclamación hasta que se firma la resolución.

El tiempo medio global de resolución ha disminuido en 10 días con respecto al año anterior, y 20 días con respecto a hace dos años, consolidando una tendencia de importante reducción de los tiempos de resolución, y ello a pesar del aumento de complejidad de los tratamientos de datos que se realizan y que a su vez determinan una mayor complejidad de las investigaciones y procedimientos de esta Agencia.

Tabla 6: Tiempo medio de resolución según el procedimiento en que se resuelve			
Tiempos medios de resolución según la fase del procedimiento (en días)	**2021**	**2022**	**Δ% anual**
Resoluciones tras las actuaciones de Traslado*	87	82	-6%
Resoluciones tras las actuaciones previas de Investigación	233	262	12%
Resoluciones en el procedimiento de Ejercicio de derechos	88	84	-5%
Resoluciones en el procedimiento Sancionador	255	242	-5%
TIEMPO MEDIO	**119**	**109**	**-9%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

3. Actuaciones realizadas

Las cifras que se muestran a continuación dan una perspectiva del total de las actuaciones realizadas en la Subdirección General de Inspección de Datos que finalizan una fase del procedimiento administrativo, pero que no necesariamente lo concluyen y, por lo tanto, no dan lugar a resoluciones. Un ejemplo de ello sería una actuación previa de investigación que da lugar a un procedimiento sancionador; esta actuación no genera una resolución y, por lo tanto, no aparece detallada en el apartado anterior, pero, sin embargo, sí implica un trabajo que es el que se indica en este epígrafe. En el caso de procedimientos de ejercicio de derechos, sancionadores o recursos de reposición, que siempre ponen fin al procedimiento administrativo y producen, por tanto, una resolución, las cifras son coincidentes con las dadas en el apartado anterior.

Se debe puntualizar que el número de reclamaciones evaluadas en la fase de análisis previo de admisibilidad puede oscilar frente al número de reclamaciones presentadas en el año, puesto que es un trámite que tiene una duración media de 24 días como se indica más adelante, por tanto se inicia el año analizando reclamaciones pendientes del último mes del año anterior, y de la misma forma se finaliza el año sin poder concluir el análisis del total de reclamaciones presentadas en las últimas semanas de año.

Se puede observar un aumento de actuaciones en las primeras etapas, consistente con el aumento de resoluciones en la fase de traslado de la reclamación al responsable o encargado. El número de actuaciones de investigación ha descendido debido a varios factores, principalmente por el aumento de resoluciones en fases anteriores, y por los criterios seguidos para su inicio: ha aumentado su rigor, acompañado de una mayor profundidad en las investigaciones. Esto último ha tenido un efecto directo sobre el porcentaje de investigaciones que culminan en procedimientos sancionadores, aumentando en 11 puntos con respecto al año anterior. La reducción en los procedimientos de derechos también deriva del aumento de resoluciones en fases previas, a lo que se añade un descenso en las reclamaciones específicamente relacionadas con el ejercicio de derechos.

Tabla 7: Actuaciones realizadas			
Número de actuaciones finalizadas según la fase del procedimiento	**2021**	**2022**	**Δ% anual**
Análisis previo de admisibilidad de reclamaciones*	14.118	14.654	4%
Actuaciones de traslado*	4.996	5.150	3%
Actuaciones previas de investigación	607	476	-22%
Procedimientos de ejercicio de derechos	351	305	-13%
Procedimientos sancionadores	585	575	-2%
Recursos de reposición	766	735	-4%
TOTAL	**21.423**	**21.895**	**2%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

3.1 Tiempos medios de tramitación

Los tiempos que aparecen en este apartado miden los tiempos medios de actuaciones de cada una de las fases individuales relacionadas con la gestión de la reclamación. Estos tiempos medios se miden en días desde el inicio de cada fase hasta su finalización.

Tabla 8: Tiempos medios de tramitación			
Tiempos medios de actuaciones realizadas en la gestión de la reclamación según la fase del procedimiento (en días)	**2021**	**2022**	**Δ% anual**
Análisis previo de admisibilidad de reclamaciones*	26	24	-9%
Actuaciones de traslado*	58	57	-2%
Actuaciones previas de investigación	205	200	-2%
Procedimientos de ejercicio de derechos	77	67	-13%
Procedimientos sancionadores	109	111	2%
Recursos de reposición	70	86	22%
TIEMPO MEDIO	**43**	**40**	**-7%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos*

4. Administraciones públicas sancionadas por incumplimiento de requerimientos y medidas

En relación con la eficacia de las actuaciones y resoluciones de la Agencia, la SGID supervisa el cumplimiento de los requerimientos de información realizados al amparo de los poderes de investigación regulados en el artículo 58.1 del RGPD, y de las medidas de adaptación a la normativa impuestas en las resoluciones de conformidad con los poderes correctivos regulados en el artículo 58.2.

La falta de respuesta a los requerimientos de información supone una infracción tipificada en el artículo 83.5.e) del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 de la LOPDGDD. Por su parte, la falta de acreditación de las medidas correctivas impuestas supone una infracción tipificada en el artículo 83.6 del RGPD, calificada igualmente como muy grave a efectos de prescripción en el artículo 72.1 de la LOPDGDD.

Dentro de las administraciones que no han cumplido las órdenes dadas desde la Agencia, merece la pena destacar aquellas entidades locales a las que se les requirió que procedieran al nombramiento del DPD. El nombramiento de DPD y su comunicación a la Agencia suponen obligaciones incluidas en el artículo 37 del RGPD para las autoridades u organismos públicos. La falta de cumplimiento supone una infracción tipificada en el artículo 83.5.b) del RGPD, y calificada como grave a efectos de prescripción en el artículo 73 de la LOPDGDD.

En la tabla siguiente se informa, para el año 2022, los responsables públicos que han sido sancionados por la Agencia por las infracciones descritas. De acuerdo con el artículo 77 de la LOPDGDD, la sanción que les corresponde es de apercibimiento.

Tabla 9: Administraciones Públicas sancionadas por incumplimiento de requerimientos y medidas correctivas

Responsable sancionado	Administración	Art. infringido	Art. de tipificación	Resolución
Empresa Municipal Transportes Urbanos, S.A. De Gijón	Administración Local	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00189-2022.pdf
Ayuntamiento de Monesterio	Administración Local	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00131-2022.pdf
Ayuntamiento de Oria	Administración Local	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00208-2022.pdf
Ayuntamiento de Burgos	Administración Local	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00120-2022.pdf

Tabla 9: Administraciones Públicas sancionadas por incumplimiento de requerimientos y medidas correctivas				
Responsable sancionado	**Administración**	**Art. infringido**	**Art. de tipificación**	**Resolución**
D.G. De La Guardia Civil	Administración General del Estado	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00327-2022.pdf
Establecimientos Residenciales para Ancianos de Asturias	Administración Autonómica	RGPD 58.2	RGPD 83.6	https://www.aepd.es/es/documento/ps-00123-2022.pdf
Ayuntamiento de Majadahonda	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00382-2022.pdf
Ayuntamiento de los Llanos De Aridane	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00384-2022.pdf
Ayuntamiento de Cambre	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00385-2022.pdf
Ayuntamiento de Arrecife	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00387-2022.pdf
Ayuntamiento de Aranda De Duero	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00366-2022.pdf
Ayuntamiento de Moncada	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00386-2022.pdf
Ayuntamiento de Algete	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00381-2022.pdf
Ayuntamiento de San Andrés Del Rabanedo	Administración Local	RGPD 37	RGPD 83.5	https://www.aepd.es/es/documento/ps-00383-2022.pdf

5. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos de Inspección se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos.

Tabla 10: Recursos recibidos			
Tipo de recurso	**2021**	**2022**	**Δ% anual**
Recursos de reposición	795	898	13%
Recursos extraordinarios de revisión	7	12	71%
Recursos contencioso-administrativos	118	115	-3%
TOTAL	**920**	**1025**	**11%**

El aumento en recursos de reposición recibidos no resulta sorprendente si se correlaciona con el aumento en el número de resoluciones emitidas por la Agencia.

Los recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla:

Tabla 11: Recursos resueltos			
Tipo de recurso	**2021**	**2022**	**Δ% anual**
Recursos de reposición	766	735	-4%
Recursos extraordinarios de revisión	7	11	57%
TOTAL	**773**	**746**	**-3%**

6. Clasificaciones

6.1 Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2022, que suponen el 80% del total de reclamaciones recibidas en el año:

Tabla 12: Reclamaciones más frecuentes

Reclamaciones planteadas con mayor frecuencia	2021	2022	% relativo	Δ% anual
TOP 10	**10.806**	**12.068**	**80%**	**12%**
Servicios de Internet	2.220	2.221	15%	0%
Videovigilancia	1.736	2.196	15%	26%
Publicidad (excepto spam)	1.528	2.001	13%	31%
Ficheros de Morosidad	1.284	1.161	8%	-10%
Reclamación de Deudas	859	913	6%	6%
Comercios, transporte y hostelería	663	908	6%	37%
Administración pública	740	797	5%	8%
Entidades financieras/acreedoras	643	769	5%	20%
Contratación fraudulenta	453	559	4%	23%
Sanidad	680	543	4%	-20%
Otros	**3.099**	**3.060**	**20%**	**-1%**
TOTAL	**13.905**	**15.128**	**100%**	**9%**

En respuesta al alto número de reclamaciones de publicidad no deseada, la AEPD ha estado trabajando junto a Autocontrol en una modificación del código de conducta sobre tratamiento de datos en la actividad publicitaria, que recoge una vía para resolver de forma más ágil las reclamaciones en materia de protección de datos y publicidad que puedan plantear los ciudadanos, y al que se han adherido los principales operadores de telecomunicaciones del país: Telefónica, Vodafone, Orange y Más móvil.

En relación con el aumento de las reclamaciones de comercios, transporte y hostelería, se puede destacar el aumento de infracciones reclamadas relacionadas con el uso de datos personales por parte de empresas de reparto y paquetería que ha tenido una repercusión importante en medios de comunicación, lo que posiblemente haya originado una mayor percepción por parte de los ciudadanos que se ha traducido en una mayor presentación de este tipo de reclamaciones.

Con respecto a la contratación fraudulenta, los sectores más afectados por las reclamaciones fueron el energético y el de las telecomunicaciones, donde se ha observado la contratación o modificación de contratos por parte de personas no autorizadas.

6.2 Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2022, que representan el 84% del total de sancionadores resueltos en el año:

Tabla 13: Procedimientos sancionadores más frecuentes

Grupo de actividad	2021	2022	% relativo	Δ% anual
TOP 10	**490**	**481**	**84%**	**-2%**
Videovigilancia	147	164	29%	12%
Servicios de internet	128	89	15%	-30%
Administración Pública	49	53	9%	8%
Brechas de datos personales	17	33	6%	94%
Spam a través de e-mail o SMS	51	29	5%	-43%
Asuntos laborales	26	27	5%	4%
Sanidad	4	25	4%	525%
Publicidad (excepto spam)	25	23	4%	-8%
Comercio, transporte y hostelería	24	21	4%	-13%
Contratación fraudulenta	19	17	3%	-11%
Otros	**95**	**94**	**16%**	**-1%**
TOTAL	**585**	**575**	**100%**	**-2%**

6.3 Reclamaciones relacionadas con la pandemia de COVID-19

Los últimos años han estado marcados por la crisis sanitaria ocasionada por la pandemia de COVID-19. En la siguiente tabla se muestra la cifra de reclamaciones relativas a tratamientos de datos personales en este contexto, donde se observa un descenso con respecto al año anterior:

Tabla 14: Reclamaciones COVID-19

Tipo de entrada	2021	2022	Δ% anual
Reclamaciones	233	157	-33%

Las cifras que se muestran a continuación dan una perspectiva del total de actuaciones realizadas en la Subdirección General de Inspección de Datos relacionadas con la COVID-19:

Tabla 15: Actuaciones COVID-19

Tipo de actuación iniciada	2021	2022	Δ% anual
Actuaciones de traslado	100	49	-51%
Actuaciones previas de investigación	25	18	-28%
Procedimientos sancionadores	30	24	-20%
Procedimientos de ejercicio de derechos	2	0	-100%
Casos de cooperación transfronteriza	1	0	-100%
Recursos de reposición	9	19	111%

7. Ámbito transfronterizo (EEE)

La aplicación del RGPD desarrolla en su capítulo VII los mecanismos de cooperación entre autoridades de control del Espacio Económico Europeo, en los que es de plena aplicación el Reglamento.

7.1 Casos transfronterizos con participación de la AEPD

En los casos con componentes transfronterizos que afectan a ciudadanos o a establecimientos de responsables en España, la AEPD participa en su resolución. Según se encuentre el establecimiento principal del responsable en España o en otro Estado miembro, en atención al mecanismo de ventanilla única, la participación será como autoridad principal o interesada respectivamente.

Tabla 16: Casos transfronterizos participados

Papel de la AEPD	2021	2022	Δ% anual
Nuevos casos liderados como autoridad principal	16	15	-6%
Nuevos casos en cooperación como autoridad interesada	304	201	-34%
TOTAL	**320**	**216**	**-33%**

7.2 Peticiones recibidas relacionadas con el procedimiento de Cooperación

Además del mecanismo de ventanilla única desarrollado en el artículo 60, el RGPD también regula otros mecanismos de cooperación en el capítulo VII. Los procedimientos de los artículos 61 y 62 pueden solicitarse incluso para casos locales.

La siguiente información recopila tanto los nuevos casos procedentes de otras Autoridades de Control, como otras solicitudes de asistencia y consulta recibidos por la AEPD, así como los proyectos de decisión analizados y participados por la AEPD.

Tabla 17: Solicitudes y decisiones recibidas en procedimientos de cooperación

Tipo de entrada	2021	2022	Δ% anual
Casos transfronterizos procedentes de otras AC	581	651	12%
Solicitudes de asistencia de otras AC	274	311	14%
Consultas de otras AC en procedimientos transfronterizos	102	48	-53%

Tabla 17: Solicitudes y decisiones recibidas en procedimientos de cooperación			
Tipo de entrada	**2021**	**2022**	**Δ% anual**
Proyectos de decisión de casos en los que la AEPD participa*	113	132	17%
Operaciones conjuntas en las que la AEPD participa	0	0	0%
TOTAL	**1.070**	**1.142**	**7%**

** Los proyectos de decisión recibidos, aun siendo emitidos por la principal, suponen el trabajo subsiguiente de negociación y consenso entre todas las autoridades participantes y requieren una gran cantidad de recursos y de esfuerzo.*

7.3 Peticiones enviadas relacionadas con el procedimiento de Cooperación

Finalmente, se muestra la misma tabla que en el apartado anterior, con la visión opuesta: los casos, solicitudes, consultas y proyectos de decisión emitidos por la AEPD hacia el resto de autoridades de control europeas.

Tabla 18: Solicitudes y decisiones remitidas en procedimientos de cooperación			
Tipo de notificación	**2021**	**2022**	**Δ% anual**
Casos transfronterizos compartidos con otras AC	30	24	-20%
Solicitudes de asistencia a otras AC	88	93	6%
Consultas a otras AC en procedimientos transfronterizos	18	18	0%
Proyectos de decisión de casos liderados por la AEPD*	23	25	9%
TOTAL	**159**	**160**	**1%**

** Los proyectos de decisión emitidos por la AEPD suponen el trabajo subsiguiente de negociación y consenso entre todas las autoridades participantes y requieren una gran cantidad de recursos y de esfuerzo.*

7.4 Grupos de trabajo internacionales

Además del trabajo de negociación y consenso en cada expediente transfronterizo en el que la Agencia ha participado, la SGID también ha estado presenta en distintas sesiones de grupos de trabajo dependientes del Comité Europeo de Protección de Datos (CEPD).

Tabla 19: Grupos europeos con participación de la SGID	
Grupo de trabajo	**Propósito**
Cooperation Expert Subgroup	Enfoque general en los procedimientos establecidos por el RGPD a los efectos del mecanismo de cooperación. Orientación sobre cuestiones de procedimiento relacionadas con el mecanismo de cooperación. Asistencia mutua internacional y otras herramientas de cooperación para hacer cumplir el RGPD fuera de la UE (artículo 50 del RGPD).
Enforcement Expert Subgroup	Analizar la necesidad de aclaraciones u orientación adicionales, basadas en experiencias prácticas con la aplicación de los capítulos VI, VII y VIII del RGPD. Análisis de las posibles actualizaciones de las herramientas existentes del subgrupo de cooperación. Seguimiento de las actividades de investigación. Preguntas prácticas sobre investigaciones. Orientación sobre la aplicación práctica del Capítulo VII del RGPD, incluidos los intercambios sobre casos concretos. Orientación sobre la aplicación del Capítulo VIII del RGPD junto con el Grupo de Trabajo sobre Multas administrativas. Procedimientos del artículo 65 y del artículo 66.
IT Users Expert Subgroup	Desarrollo y prueba de herramientas informáticas utilizadas por el CEPD con un enfoque práctico. Recopilación de comentarios sobre el sistema de TI por parte de los usuarios. Adaptación de los sistemas y manuales. Discutir otras necesidades de negocio, incluidos los sistemas de teleconferencia y videoconferencia.
Taskforce on Administrative Fines	Elaboración de directrices para la armonización del cálculo de las multas.
Cookie Banner Taskforce	Intercambiar puntos de vista sobre el análisis jurídico y las posibles infracciones. Prestar apoyo a las actividades a nivel nacional. Agilizar la comunicación.
101 Complaints Taskforce	Examinar las reclamaciones presentadas tras la sentencia del TJUE Schrems II y garantizar una estrecha cooperación entre los miembros del CEPD.

Tabla 19: Grupos europeos con participación de la SGID	
Grupo de trabajo	**Propósito**
Support Pool of Experts	Iniciativa estratégica del CEPD, que ayuda a las autoridades de supervisión a aumentar su capacidad para supervisar y hacer cumplir la salvaguarda de los datos personales.
Sistema de Información Schengen –SIS-	Reunión de coordinación de Sistema de Información Schengen de segunda generación –SIS II-con las autoridades nacionales SIS II en el marco de la planificación de la evaluación Schengen.

8. Multas

8.1 Evolución de las multas impuestas

Las siguientes cifras hacen referencia a las sanciones económicas impuestas en resolución definitiva, con independencia de su estado de ejecución y recaudación:

Tabla 20: Volumen de multas			
Evolución de las multas impuestas	**2021**	**2022**	**Δ% anual**
Número de multas	258	378	47%
Importe total	35.074.800	20.775.361	-41%

Según el portal *www.enforcementtracker.com* [1] y para el ejercicio de 2022:

- La AEPD ha declarado el **40,2 % de las multas** impuestas en el Espacio Económico Europeo
- El importe total de multas impuestas por la AEPD que representa el **2,5 % del importe total de sanciones** declaradas en el Espacio Económico Europeo.

Se observa un aumento del número de multas impuestas, si bien el importe total se reduce, debido a una disminución en el número de grandes procedimientos resueltos durante este último año frente a lo sucedido durante el año 2021 . En este sentido, las multas superiores al millón de euros en resoluciones firmadas en 2022 que han devenido firmes y ejecutivas se detallan a continuación:

[1] *El portal www.enforcementtracker.com no es una fuente oficial del Comité Europeo de Protección de Datos ni de ninguna autoridad de protección de datos. Se trata de una iniciativa privada que recoge datos de sanciones y multas a partir de la información publicada por las diferentes autoridades de protección de datos europeas, por lo que puede haber sanciones impuestas por las autoridades que no figuren en dicho portal.*

Tabla 21: Multas superiores al millón de euros		
Responsable	**Infracción**	**Multa**
CAIXABANK, S.A.	Artículo 6.1 del RGPD Artículo 7 del RGPD	2.100.000 €
AMAZON ROAD TRANSPORT SPAIN, S.L.	Artículo 6.1 del RGPD Artículo 10 del RGPD	2.000.000 €
GOOGLE LLC	Artículo 6.1 del RGPD Artículo 17 del RGPD	10.000.000 €

8.2 Áreas con mayor importe global de multas

La siguiente tabla desglosa las 6 áreas de actividad con mayor importe en sanciones en 2022:

Tabla 22: Desglose de multas por temas				
Importe de multas en euros según el tema	**2021**	**2022**	**% relativo**	**Δ% anual**
Seis temas con mayor importe total en 2022	**22.329.400**	**18.143.401**	**87%**	**-19%**
Servicios de Internet	150.300	11.492.201	55%	7546%
Publicidad (excepto SPAM)	8.659.200	2.291.800	11%	-74%
Asuntos laborales	2.625.900	2.198.800	11%	-16%
Brechas de datos personales	720.000	821.800	4%	14%
Contratación fraudulenta	3.674.000	706.800	3%	-81%
Telecomunicaciones	6.500.000	632.000	3%	-90%
Otros	**12.745.400**	**2.631.960**	**13%**	**-79%**
TOTAL	**35.074.800**	**20.775.361**	**100%**	**-41%**

El importe correspondiente al grupo de servicios de Internet y su gran aumento con respecto al año anterior, obedece a la multa indicada en el apartado anterior a Google LLC de 10 millones de euros.

Así mismo, la bajada en el importe de las multas de telecomunicaciones en un 90% se debe a que durante el año 2021 se finalizaron procedimientos de importe significativo contra los principales operadores de telecomunicaciones.

Anexo A: Datos del Canal Prioritario

En 2019 la AEPD creó un sistema específico para perseguir la difusión ilegítima de contenidos especialmente sensibles de menores y otros colectivos vulnerables, conocido como Canal Prioritario. Adicionalmente, a efectos de facilitar la comunicación de este tipo de casos a los menores de edad, se flexibilizaron los requisitos de sus comunicaciones, facilitando un medio de contacto basado en un formulario abierto, sin necesidad de presentar certificado digital.

A.1 Entradas recibidas a través del Canal Prioritario

A continuación, se muestran las entradas recibidas por los dos canales referidos anteriormente.

Tabla 23: Entradas recibidas por el Canal Prioritario

Tipo de entrada	2021	2022	Δ% anual
Reclamaciones presentadas ante la AEPD	162	255	57%
Comunicaciones del canal de menores (14-18 años)	215	167	-22%
TOTAL	**377**	**422**	**12%**

A.2 Entradas tramitadas con carácter de urgencia tras el análisis de la Agencia

Cada entrada que llega a través del Canal Prioritario se analiza en profundidad para determinar si el caso reúne las características para ser tratado como sensible, en cuyo caso se procede a su tramitación con carácter de urgencia. En el resto de casos, también se puede continuar su tramitación, aunque ya por la vía ordinaria y sin el carácter de urgencia, debido a que, tras el análisis de las mismas, se observa que no tienen relación con contenidos especialmente sensibles.

Tabla 24: Entradas tratadas por vía urgente

Tipo de entrada	2021	2022	Δ% anual
Reclamaciones recibidas por el Canal Prioritario que han tenido una tramitación urgente	16	33	106%
Reclamaciones recibidas por canales ordinarios que han tenido una tramitación urgente	8	10	25%
Comunicaciones del canal de menores (14-18 años) que han tenido una tramitación urgente	5	17	240%
TOTAL	**29**	**60**	**107%**

A.3 Intervenciones realizadas con carácter de urgencia

Cuando se determina la naturaleza especialmente sensible de los datos personales divulgados y la afectación grave a la intimidad de las personas, puede resultar necesario y proporcionado realizar una intervención de urgencia para adoptar medidas provisionales que permitan salvaguardar el derecho fundamental a la protección de los datos personales de los afectados.

En tales casos, se requiere a los proveedores de servicios correspondientes la retirada de los contenidos sensibles con la mayor inmediatez posible. En la siguiente tabla se muestra el número de intervenciones realizadas con carácter de urgencia y los casos en los que han resultado ser eficaces, retirándose los contenidos expuestos. Las intervenciones que no han resultado eficaces demuestran las dificultades de retirada de contenidos cuando los responsables se localizan en terceros países.

Tabla 25: Intervenciones de retirada de contenidos

Tipo de Actuación	2021	2022	Δ% anual
Intervenciones con carácter de urgencia para la retirada de contenidos	31	51	65%
Intervenciones que han resultado eficaces	25	46	84%

Anexo B: Mejora Productividad. Comparación con la implantación del Teletrabajo.

La productividad de la actividad global de la Subdirección General de Inspección de Datos se puede medir en base a indicadores como la *actividad de resolución* y el *tiempo de resolución*. La *actividad de resolución* se puede contabilizar, por un lado, de manera absoluta, mediante el *número de entradas resueltas* a lo largo de un ejercicio, y, por otro lado, mediante la tasa de resolución, que pone en relación las entradas resueltas y las que han sido recibidas en el mismo período. Una tasa de resolución del 100%, indica que se está dando respuesta a todo el volumen de trabajo que se recibe. El *tiempo de resolución*, por su parte, es una medida única que indica el tiempo medio desde que un nuevo caso tiene entrada en la Agencia hasta que se firma la resolución que pone fin al mismo.

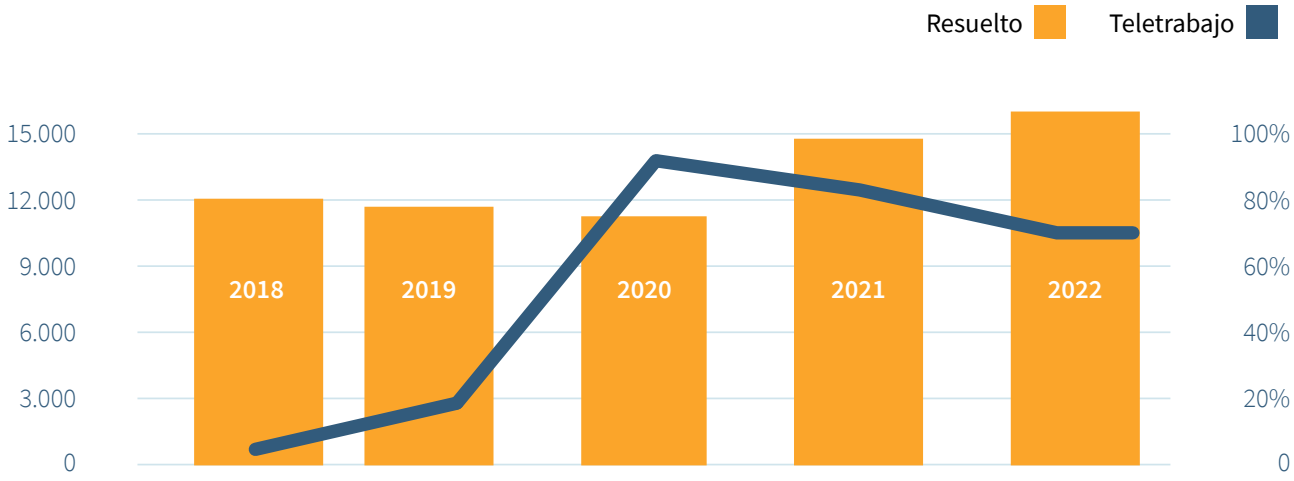
A continuación, se mostrará la evolución de los indicadores señalados desde 2018, año en que comienza la plena aplicación del RGPD, que supuso un cambio en la estructura y en el procedimiento de trabajo de la SGID, por lo que los datos de estos años son plenamente comparables.

Debe tenerse en cuenta que es durante el año 2018 cuando se lanza sistemáticamente el programa de teletrabajo, por lo que en los gráficos se incluirá también el grado de penetración del teletrabajo. A los efectos de este informe, la penetración del teletrabajo se estima como las jornadas de teletrabajo de todo el personal realizadas sobre el total de jornadas de trabajo, y por tanto para su cálculo se considera tanto el % de personal acogido al régimen de teletrabajo como el número de días por semana que realiza en el sistema de teletrabajo (así, por ejemplo, un 100% de la plantilla realizando tres días por semana de teletrabajo, supone un 60% de teletrabajo).

B.1 Actividad de resolución

La siguiente gráfica de actividad muestra el *número de entradas resueltas*, confrontado con la penetración del teletrabajo. Durante trece meses, entre marzo de 2020 y abril de 2021, la práctica totalidad del personal estuvo trabajando en remoto la totalidad de su jornada. En la segunda parte de 2021 y 2022, el régimen de teletrabajo se ha mantenido estable. El grado de teletrabajo no solo permitió continuar con la actividad durante los peores meses de la pandemia, sino que demostró sostener una productividad muy alta en 2021 y 2022. En este año se han resuelto más de 15.000 reclamaciones, y más de 840 casos procedentes de otros tipos de entradas (casos procedentes de otras AC del EEE, brechas de seguridad y casos del canal prioritario de menores), cifras sin precedentes. Esto supone un incremento de alrededor del 40% en comparación con los años anteriores a 2018.

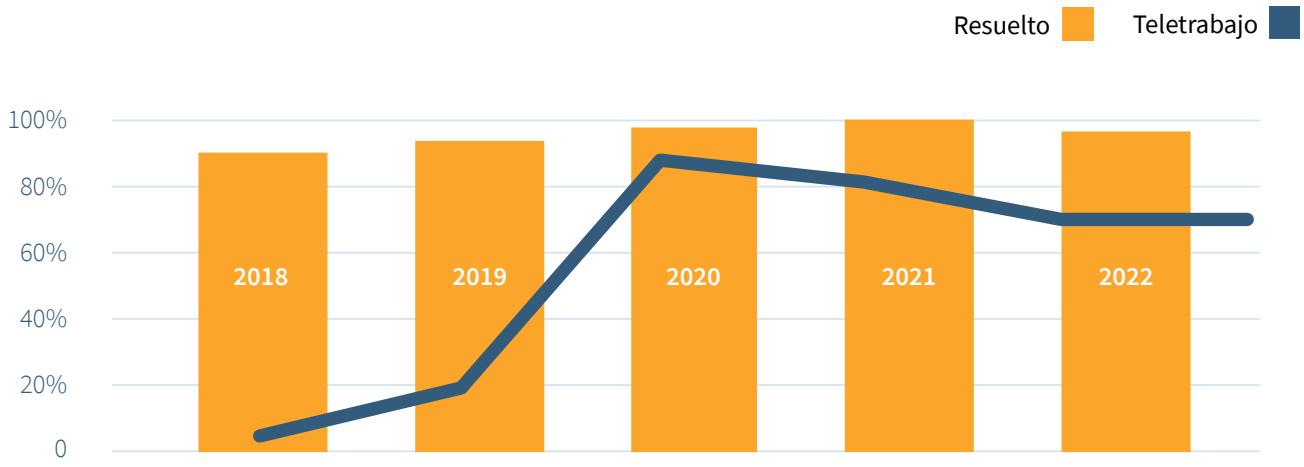
Tabla 26: Entradas resueltas y teletrabajo



Al aumento en los casos resueltos se suma un incremento de la envergadura y complejidad que tienen, como demuestra el hecho de que el importe medio de las multas impuestas en 2021 y 2022 sea varias veces superior al importe medio de los años previos al RGPD.

A continuación, se muestra un gráfico similar, pero usando para mostrar la actividad el indicador de la *tasa de resolución* (entradas resueltas en relación con las recibidas), obteniendo una lectura similar a la destacada anteriormente, las mejoras en tasa de resolución coinciden con años con una alta penetración de teletrabajo.

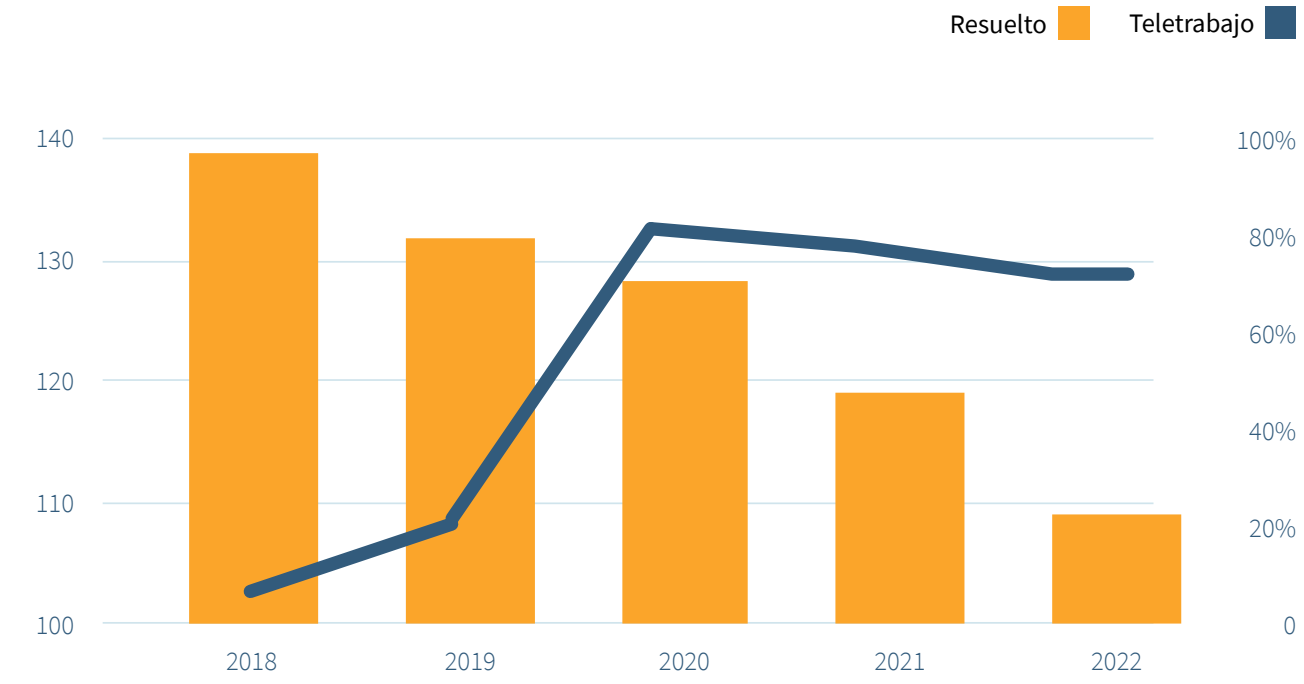
Tabla 27: Tasa de resolución y teletrabajo



B.2 Tiempo de resolución

Por lo que respecta al tiempo de resolución, se ha experimentado una reducción sostenida desde 2018, reduciendo por tanto el plazo en el que el ciudadano obtiene una respuesta a su caso. Esta tendencia es paralela al aumento de penetración del teletrabajo, reduciéndose año tras año a valores mínimos desde que se analiza este indicador. Así, como se observa a continuación, se ha podido reducir el tiempo medio de 139 a 109 días en solo cuatro años.

Tabla 28: Tiempo de resolución y teletrabajo

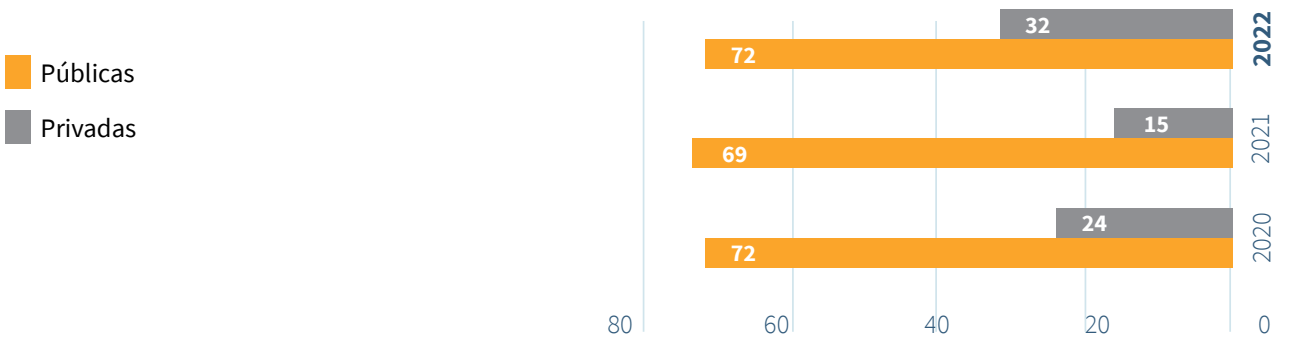


2. Gabinete Jurídico

Consultas

	Administraciones Públicas
AGE	57
CCAA	2
Entidades locales	0
Otros	13
TOTAL 1	**72**
	Consultas Privadas
Asociaciones y Fundaciones	3
Empresas	28
Particulares	1
Sindicatos	0
Otros	0
TOTAL 2	**32**
TOTAL	**104**

Evolución de consultas



Evolución de consultas por sectores (2021-2022)		
	2021	2022
Administraciones Públicas	62	**72**
Telecomunicaciones	5	**24**
Sanidad / Salud Pública	6	**1**
Particulares	0	**1**
Asesoría y consultoría	0	**0**
Sindicatos	0	**0**
Servicios informáticos	0	**0**
Asociaciones empresariales	1	**0**
Asociaciones y fundaciones	1	**3**
Solvencia patrimonial	0	**0**
Servicios	2	**0**
Agua y energías	0	**0**
Seguridad	0	**0**
Transporte	0	**0**
Servicios financieros	3	**1**
Investigación	0	**1**
Servicios de mensajería	1	**0**
Seguros	0	**1**
Partidos políticos	0	**1**
Comunidades de propietarios	2	**0**
Industria y construcción	1	**0**
Educación	0	**2**

Nota: Existen consultas que versan sobre más de un sector y son clasificadas en el que más relevancia tengan. Asimismo otras categorías están en desuso y tienden a desaparecer se mantienen en términos comparativos con el ejercicio anterior. Se han añadido nuevas que en el ejercicio anterior tienen 0.

Evolución de consultas por materias (2021-2022)		
	2021	2022
Conceptos Generales*	52	**49**
Ámbito de Aplicación	6	**4**
Licitud	8	**11**
Derecho de Información y Transparencia	4	**26**
Finalidad	6	**3**
Minimización y Proporcionalidad	13	**16**
Exactitud/Calidad de datos	7	**6**
Plazo de Conservación	2	**1**
Integridad y Confidencialidad	2	**0**
Consentimiento	11	**10**
Interés Legítimo	0	**1**
Responsable	5	**4**
Encargado	7	**1**
Corresponsable	0	**0**
Derechos	4	**3**
Derecho a información y Transparencia	5	**0**
Tratamientos Videocámaras	1	**0**
Categorías Especiales de datos	13	**14**
Seguridad en el Tratamiento	4	**3**
Responsabilidad Activa	7	**0**
Delegado Protección Datos	5	**3**
Gestión Riesgo y Evaluación de Impacto	3	**2**
Transferencias Internacionales	1	**0**
Transparencia y acceso a registros públicos	5	**0**

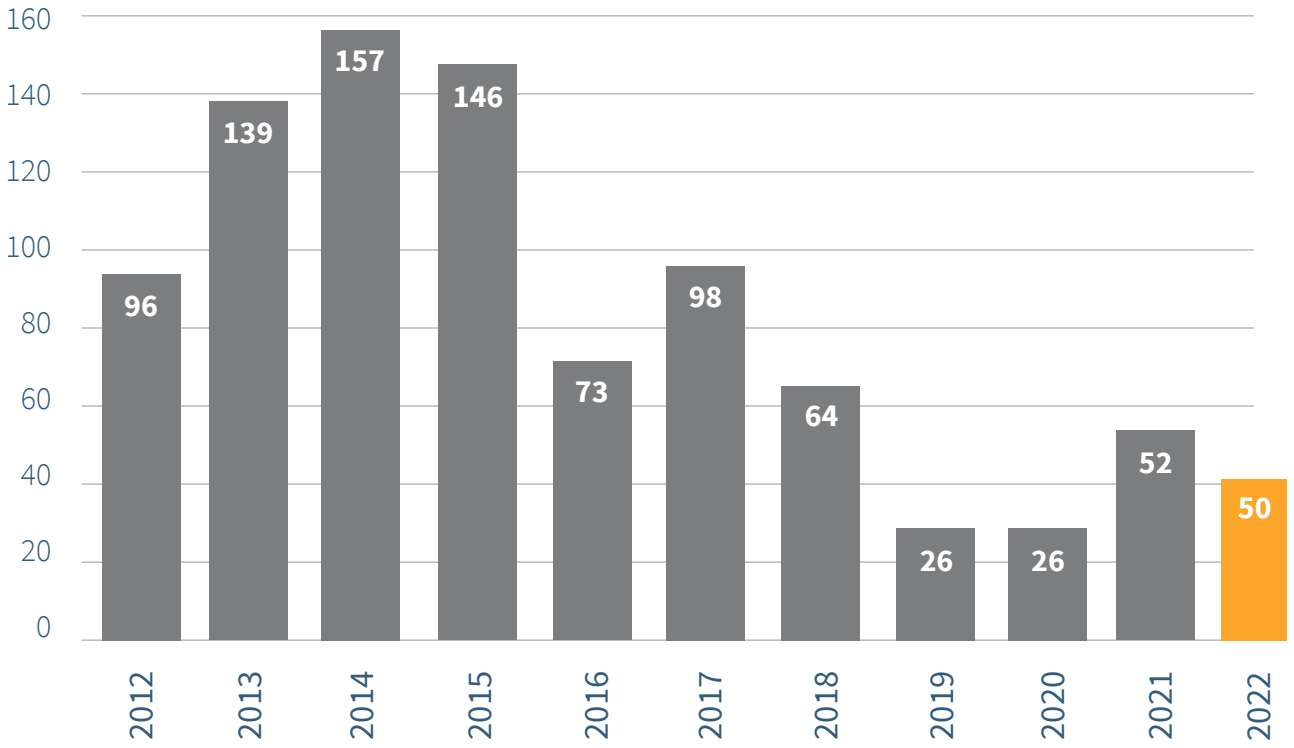
** **Conceptos Generales:** se incluyen aquí las consultas sobre proyectos de disposiciones generales.*

Evolución de consultas por materias (2021-2022)		
	2021	2022
Telecomunicaciones	4	**24**
Menores	0	**0**
Administración electrónica	1	**0**
Estadística	1	**0**
Códigos de Conducta	0	**3**

Nota: Existen consultas que versan sobre más de una materia y que por su relevancia constan en más de un apartado.

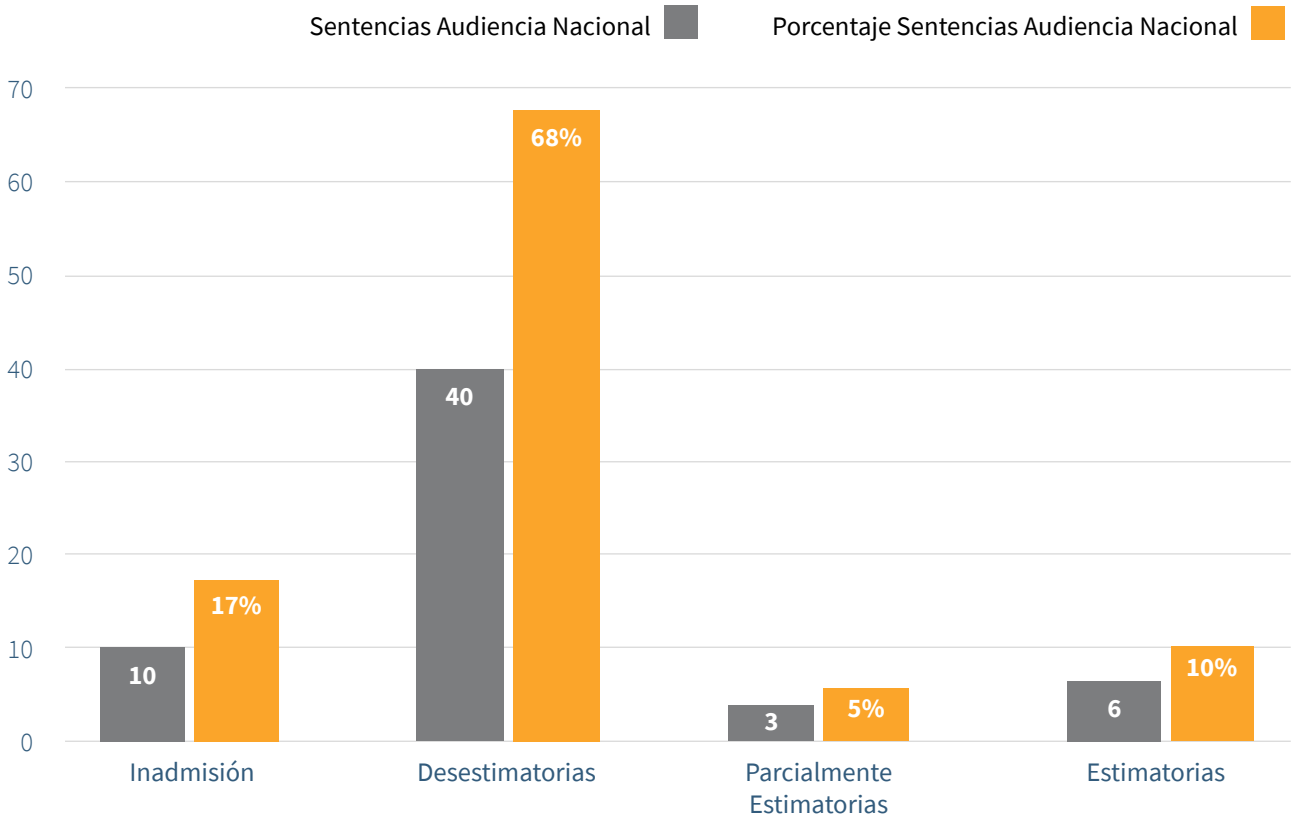
Evolución de informes preceptivos a disposiciones generales (2012-2022)

Disposiciones Generales



Evolución informes preceptivos (2012-2022)			
Año	Disposiciones generales	RD 424/2005	Total
2012	96	27	174
2013	139	21	162
2014	157	23	182
2015	146	15	173
2016	73	23	97
2017	98	28	126
2018	64	24	88
2019	64	12	76
2020	26	15	41
2021	52	5	57
2022	**50**	**24**	**74**

Sentencias Audiencia Nacional 2022

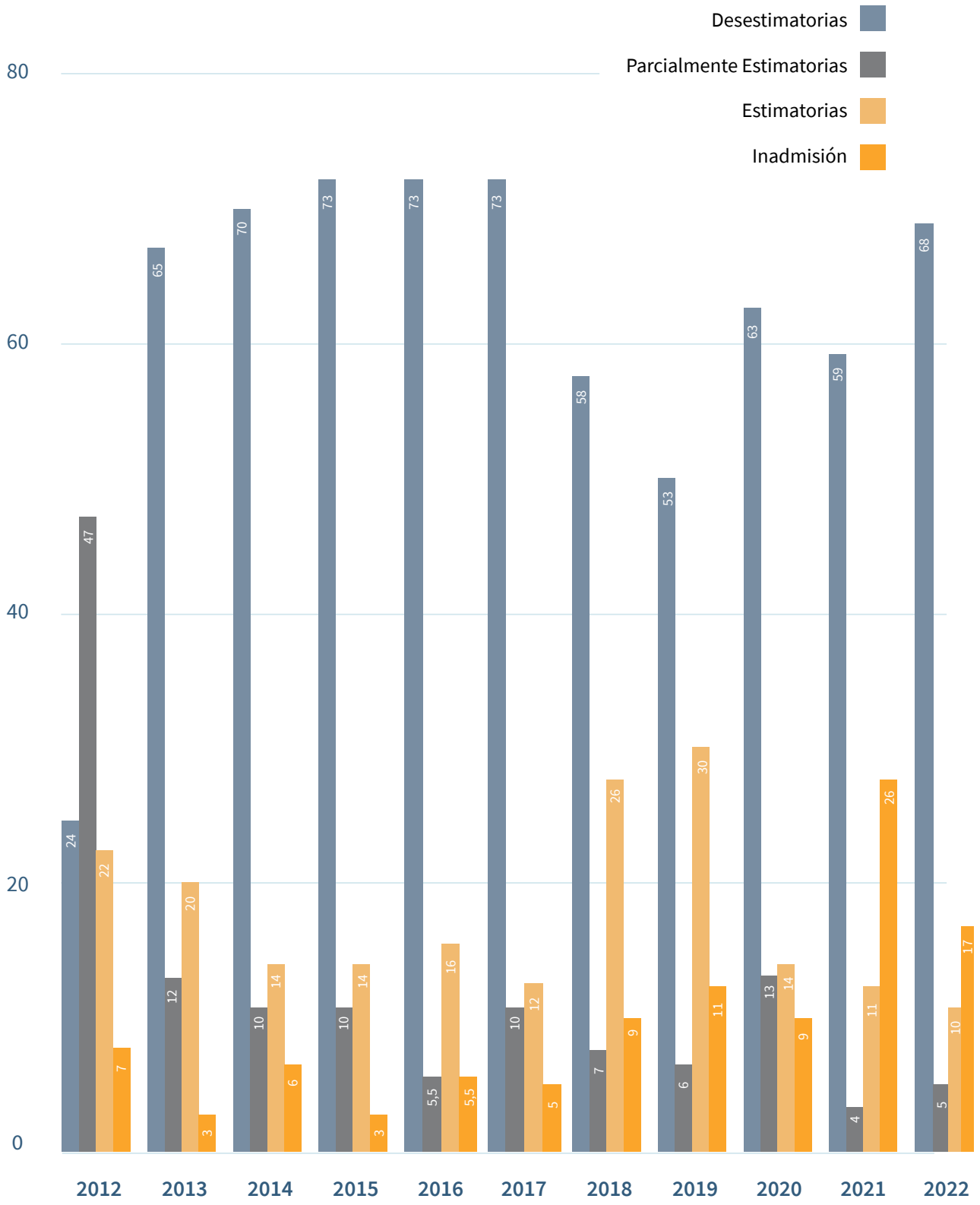


TOTAL Sentencias Audiencia Nacional 2020	**59**

Sentencias Tribunal Supremo (2022)

Evolución por sentido del fallo en porcentajes (2012-2022)				
Ejercicio (año)	Desestimatorias	Parcialmente Estimatorias	Estimatorias	Inadmisión
2012	24	47	22	7
2013	65	12	20	3
2014	70	10	14	6
2015	73	10	14	3
2016	73	5,5	16	5,5
2017	73	10	12	5
2018	58	7	26	9
2019	53	6	30	11
2020	63	13	14	9
2021	59	4	11	26
2022	**68**	**5**	**10**	**17**

Evolución por sentido del fallo en porcentajes (2012-2022)



Comparativa por sector recurrente (2021-2022)		
	2021	2022
Particulares	41	**50**
Banca y seguros	7	**1**
Telecomunicaciones	5	**5**
Solvencia patrimonial y crédito	3	**1**
Distribución y venta	3	**2**
Agua y energía	3	**4**
Administraciones Públicas	2	**2**
Otros	2	**2**
Asociaciones y sindicatos	2	**0**
Sociedad de la información	2	**0**
Publicidad y prospección comercial	1	**2**
Salud	0	**0**
TOTAL	**71**	**69**

Nota: Se incluyen todo tipo de resoluciones de la AN y el TS, sentencias, autos, providencias, diligencias de ordenación, etc.

3. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano[1]				
	2020	2021	2022	% 2021-2022
Presenciales	310[2]	64[3]	110	71,8%
Telefónicas	41.096	41.022	42.562	3,75%
Sede electrónica y email	8.280	3.779	3.766[4]	-0,3%
TOTAL	**49.686**	**44.865**	**46.438**	**3.50%**

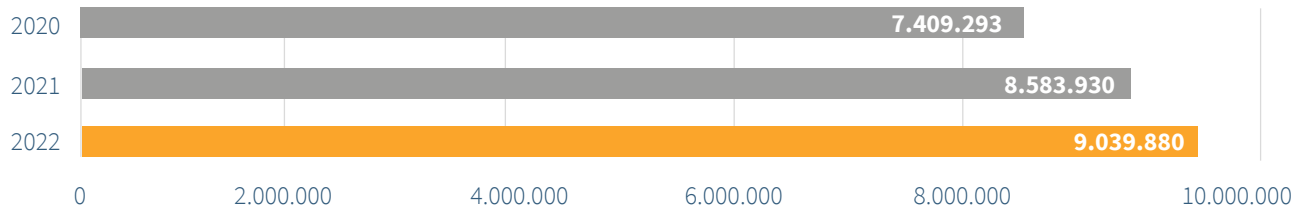
[1]Desde esta área se han atendido 86 requerimientos y solicitudes de información procedentes de Juzgados y Tribunales.

[2]Del 1 de enero 2020 al 13 de marzo 2020 - La atención presencial dejó de prestarse el 16 de marzo de 2020.

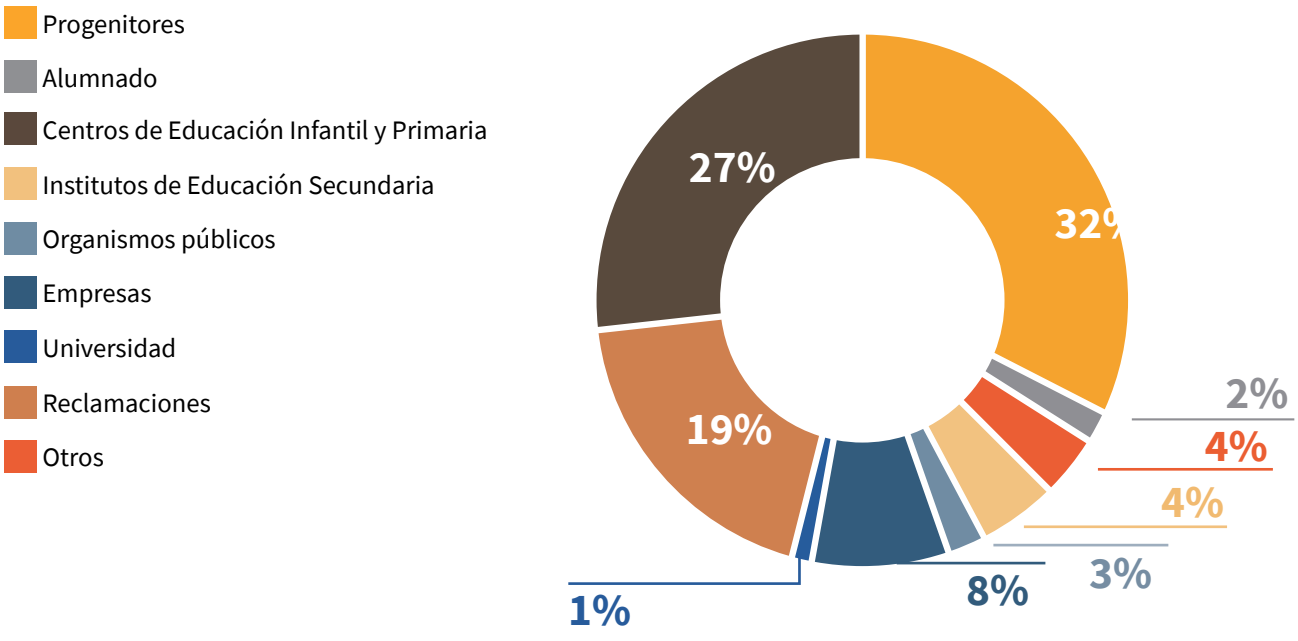
[3]Se reanuda la atención presencial el día 19 de abril de 2021, con cita previa.

[4]Incluye las Quejas y Sugerencias (107) atendidas conforme al Real Decreto 51/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado y las consultas del canal DPD (695).

Comparativa de visitas a la web (*www.aepd.es*)				
	2020	2021	2022	% 2021-2022
Nº de visitas	7.409.293	8.583.930	9.039.880	5.31%



Consultas especializadas sobre el tratamiento de datos de menores				
	2020	2021	2022	% 2021-2022
Teléfono	552	564	1.243	120%
WhatsApp	424	624	607	-2,7%
Correo-e	241	366	362	-1%
Sede electrónica	176	235	156	-33,4%
TOTAL	**1.393**	**1.789**	**2.368**	**32,4%**



[5]*Este epígrafe sólo recoge las consultas recibidas por Canal Joven y Sede electrónica.*

Accesos a la web www.tudecideseninternet.es			
	2020	2021	2022[6]
Visitantes distintos[7]	60.478	47.130	38.482
Números de visitas[8]	92.196	82.589	70.237

[6] Datos hasta el 16 de noviembre, fecha en la que se realiza la migración del portal "tudecideseninternet" alojado en el Mº de Educación y Formación Profesional, al servidor de la AEPD.

[7] Visitante que ha solicitado al menos una página. Si este visitante ingresa numerosas veces sólo contará como una.

[8] Número de visitas realizadas por todos los visitantes. Si cada visitante tiene una sesión, cada visita que realice aumentará este contador.

Accesos a la web www.tudecideseninternet.es[9]	
	2022
Número de visitas	10.768

[9] Desde el 17 de noviembre, el portal "tudecideseninternet" se encuentra en el servidor de la AEPD.

Accesos a otras webs temáticas	
	2022
Un móvil es más que un móvil[10]	30.398
Canal Prioritario[11]	61.238

[10] Desde el 10 de noviembre. Se completa con las descargas de la guía "Más que un móvil" que han sido 26.065 en el mismo periodo (ver cuadro Descargas de Guías).

[11] Independientes de las reclamaciones.

Canal del DPD[12]			
	2020 (desde 1/11)	2021	2022
Consultas	200	669	695

[12] *El Canal del DPD sustituyó al Canal Informa el 1 noviembre 2020*

Informe de Accesos a FAQ	
Temas de consulta	Nº de visitas
Reglamento General de Protección de Datos. (RGPD)	63.026
Cuestiones sobre la Sede Electrónica	36.708
Responsable, Encargado y Delegado de Protección de Datos	30.855
Menores y educación	28.285
Tus Derechos (Información, Acceso, Rectificación y Cancelación)	21.082
Transferencias internacionales, BCR y Códigos de conducta	19.411
Comunidades de Propietarios	18.698
Tratamiento de datos en el Ámbito Laboral	17.861
Videovigilancia	17.675
Solvencia patrimonial (ficheros de morosos)	13.751
Salud y coronavirus	12.975
Redes sociales, difusión ilegítima de contenidos sensibles	12.203
Reclamaciones ante AEPD y ante otros organismos competentes	10.759
Transparencia y protección de datos	9.058
Publicidad no deseada	4.464
Procesos electorales	2.801
Total	**319.612**

Sección Salud y Protección de Datos[13]	
Temas de consulta	Nº de visitas
Tus derechos en relación con tus datos de salud	5.740
Guías, informes del Gabinete Jurídico y consultas de Delegados de Protección de Datos sobre salud	4.706
Protección de datos personales en la pandemia de COVID-19	25.164
Investigación sanitaria y ensayos clínicos	2.904
Principales reclamaciones en materia de salud	5.923
Brechas de datos personales en el sector de la salud	3.153
Total	**47.590**

[13] *Disponible en la web desde el 4 de mayo de 2022*

Sección Administraciones Públicas[14]	
Temas de consulta	Nº de visitas
Régimen general de los tratamientos realizados por las AAPP	1.279
Guías, informes y documentos sobre los tratamientos de datos personales de las AAPP	1.749
Instrucciones e informes	1.031
Consultas más relevantes atendidas a través del Canal del DPD	2.028
Brechas de datos personales	721
Resoluciones relevantes sobre tratamientos de las AAPP	1.717
Herramientas y Canal del DPD	829
Total	**9.354**

[14] *Disponible en la web desde el 3 de octubre de 2022*

Temas más consultados en la atención telefónica					
Orden	Temas de consulta	2021	%	2022	%
1	Reclamaciones	10.441	24,63	10.023	23,55
2	Reglamento general de protección de datos (RGPD)	6.899	16,27	7.272	17,08
3	Derechos	5.603	13,21	5.294	12,43
4	Videovigilancia	3.061	7,22	3.431	8,06
5	Ficheros de solvencia patrimonial	2.681	6,32	1.939	4,55
6	Cuestiones técnicas de la sede electrónica	1.831	4,32	1.220	2,86
7	Herramienta FACILITA	1.438	3,39	1.254	2,94
8	Delegados de Protección de Datos	1.342	3,16	1.137	2,67
9	Comunidades de propietarios	1.038	2,44	1.043	2,45
10	Tratamiento de datos en el ámbito laboral	543	1,28	468	1,09
11	Transparencia y Protección de Datos	150	0,35	91	0,21
12	Otras cuestiones	4.578	10,80	3.476	8,16

Otros contenidos	
Guías	**Descargas**
Guía sobre el uso de videocámaras para seguridad y otras finalidades	**64.403**
Guía sobre el uso de las cookies	**51.410**
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	**42.819**
Guía para la gestión y notificación de brechas de seguridad	**42.422**
La protección de datos en las relaciones laborales	**38.299**
Protección de datos y Administración Local	**38.148**
Guía para el ciudadano	**35.040**
Guía para el cumplimiento del deber de informar	**34.903**
Guía de protección de datos y prevención de delitos	**34.356**
Guía para el responsable de tratamiento de datos personales	**34.173**
Guía de Privacidad y Seguridad en Internet	**34.062**
Guía para pacientes y usuarios de la Sanidad	**33.872**
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	**27.385**
La guía que no viene con el móvil	**26.065**
Hoja de ruta para garantizar la conformidad con la normativa de protección de datos	**19.294**
Orientaciones y Garantías en los procedimientos de anonimización	**19.089**
Guía de Protección de Datos por Defecto	**18.836**
Compra segura en INTERNET - Guía Práctica	**17.754**
Guía para profesionales del sector sanitario	**15.778**
Listado de elementos para el cumplimiento normativo	**13.290**
Guía de administradores de fincas	**13.228**

Otros contenidos	
Guías	**Descargas**
Guía de Privacidad desde el diseño	**12.465**
Drones y Protección de Datos	**11.434**
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	**9.994**
Guía de Tecnologías y Protección de Datos en las AA.PP.	**9.863**
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial	**9.014**
10 malentendidos relacionados con la anonimización	**7.955**
Requisitos para Auditorías de Tratamientos que incluyan IA	**7.722**
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube...	**7.530**
Guía de Privacidad desde el diseño (versión en inglés)	**7.446**
Guía sobre el uso de las cookies (versión en inglés)	**6.444**
Código de buenas prácticas en protección de datos para proyectos Big Data	**6.216**
Guía para clientes que contraten servicios de Cloud Computing	**5.001**
Cómo gestionar una fuga de información en un despacho de abogados	**4.758**
La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD	**4.242**
Guía de protección de datos y prevención de delitos: fichas prácticas	**4.211**
10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)	**3.777**
RGPD compliance of processings that embed Artificial Intelligence An introduction	**3.373**
Orientaciones para prestadores de servicios de Cloud Computing	**3.186**
Audit Requirements for Personal Data Processing Activities involving AI	**3.165**
Guidelines for Data Protection by Default	**2.865**
Risk Management and Impact Assessment in the Processing of Personal Data	**2.659**

Otros contenidos	
Guías	**Descargas**
Drones y Protección de Datos (versión en inglés)	**2.136**
Technologies and Data Protection in Public Administrations	**1.789**
Criterios de acreditación para los organismos de supervisión de códigos de conducta	**1.590**
10 Misunderstandings about Machine Learning	**1.110**
10 Misunderstandings Related to Anonymisation	**1.035**
Roadmap to ensure compliance with data protection regulation	**1.018**
Infografías	**Descargas**
Cuáles son tus derechos de protección de datos	**44.048**
Cuándo y cómo se debe comunicar una brecha de datos a los afectados	**25.104**
Actuación del coordinador/a de bienestar y protección del alumnado	**23.524**
Mapa de referencia para tratamientos que incluyen Inteligencia Artificial	**19.753**
Decálogo para el personal sanitario y administrativo	**9.471**
Responsabilidad de los y las menores (y de sus padres y madres) por los actos cometidos en Internet	**8.735**
Adaptación al RGPD del Sector Privado	**5.388**
Información sobre consentimiento para tratar datos personales de menores de edad	**5.371**
Quién es quién en el tratamiento de datos personales en tu centro educativo	**4.240**
Infografía Protección del menor en Internet	**3.458**
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	**2.713**
Riesgos del internet de las cosas en el hogar	**2.490**
Infografía: Medidas para minimizar el seguimiento en internet	**2.379**
10 consejos básicos para comprar en internet de forma segura	**2.260**

Otros contenidos	
Infografías	**Descargas**
Los derechos que tienes para proteger tus datos personales	**2.242**
Adaptación al RGPD de las Administraciones Públicas	**2.055**
Recomendaciones en la contratación a distancia de servicios de telecomunicaciones y energía	**1.470**
Cómo evitar la publicidad no deseada	**1.428**
Protección de datos en vacaciones	**1.332**
Juguetes conectados	**1.260**
Notas técnicas	**Descargas**
El uso de las tecnologías en la lucha contra el COVID19	**35.272**
Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo	**18.492**
14 equívocos con relación a la identificación y autenticación biométrica	**8.590**
Introducción a las tecnologías 5G y sus riesgos para la privacidad	**7.674**
Protección del menor en Internet	**5.982**
La K-anonimidad como medida de la privacidad	**5.585**
El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles	**5.014**
Medidas para minimizar el seguimiento en internet	**4.577**
Recomendaciones para el despliegue de aplicaciones móviles en el acceso a espacios públicos	**3.229**
K-anonymity as a privacy measure	**2.487**
Privacidad en DNS	**1.822**
Control del usuario en la personalización de anuncios en Android	**1.632**
The duty to inform and other accountability measures for mobile devices	**1.629**
Acceso de aplicaciones a la pantalla en dispositivos Android	**1.385**

Otros contenidos	
Notas técnicas	**Descargas**
Measures to minimise internet tracking	**1.189**
User controls for ad personalisation on Android	**1.139**
Technologies in the fight against COVID19	**1.026**
14 misunderstandings with regard to biometric identification and authentication	**974**
Guidelines for social distance and access control apps due to COVID-19	**963**
Avance del estudio de IMDEA NETWORKS y UC3M: “Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios”	**924**
DNS Privacy	**817**
Preview of "An Analysis of Pre-installed Android Software and Risks for Users' Privacy", an study by IMDEA NETWORKS and UC3M	**815**
Introduction to 5G technologies and their risks in terms of privacy	**751**
Recommendations to protect personal data in situations of mobility and telecommuting	**670**
Access to applications on the screen for Android devices	**518**
Otras publicaciones	**Descargas**
FAQ sobre el COVID-19	**10.026**
Introducción al hash como técnica de seudonimización de datos personales	**8.276**
Preguntas frecuentes sobre la anulación del Escudo de Privacidad	**7.749**
Fingerprinting o Huella digital del dispositivo	**6.693**
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	**6.467**
Orientaciones para la aplicación de la disposición adicional octava y la disposición final duodécima de la LOPDGDD	**6.016**
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas	**5.488**
LOPD: Novedades para el Sector Público	**5.061**
Adecuación a la normativa a ‘coste cero’ y otras prácticas fraudulentas	**4.925**

Otros contenidos	
Otras publicaciones	**Descargas**
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	**4.339**
Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado	**3.813**
LOPD: Novedades para los ciudadanos	**3.669**
Plan de inspección de oficio de la atención sociosanitaria	**3.524**
LOPD: Novedades para el Sector Privado	**3.363**
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	**3.351**
Fingerprinting o Huella digital del dispositivo (Versión en Inglés)	**3.208**
Plan de inspección sectorial de oficio Hospitales Públicos	**2.230**
Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía	**1.822**
Introduction to the Hash function as a personal data pseudonymisation technique	**1.815**
Análisis de los flujos de información en Android	**1.808**
FAQ about the COVID-19	**1.512**
25 años de la Agencia Española de Protección de Datos	**1.287**
Análisis de los flujos de información en Android (Versión en Inglés)	**1.023**
Encuesta sobre el grado de preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	**843**
Guidelines for Implementation of the Eighth Additional Provision and Twelfth Final Provision of the LOPDGDD	**681**
Memorias	**Descargas**
Memoria de Responsabilidad Social 2021	**15.788**
Memoria AEPD 2021	**13.260**

Pacto digital para la protección de personas

Pacto digital para la protección de personas	
	2022
Entidades adheridas (totales)	445

Códigos de Conducta [15]

	Aprobados	Modificados	Inadmitidos	En tramitación	Iniciativas
2021	2	1	0	14*	4
Total códigos de conducta aprobados					**3**

* *Cuatro códigos son de carácter transnacional, en uno de ellos actuamos como correvisores.*

[15] *En el proceso de Códigos de Conducta se mantienen reuniones con todos los promotores, con el fin de aclarar las cuestiones relativas a la tramitación de los Códigos.*

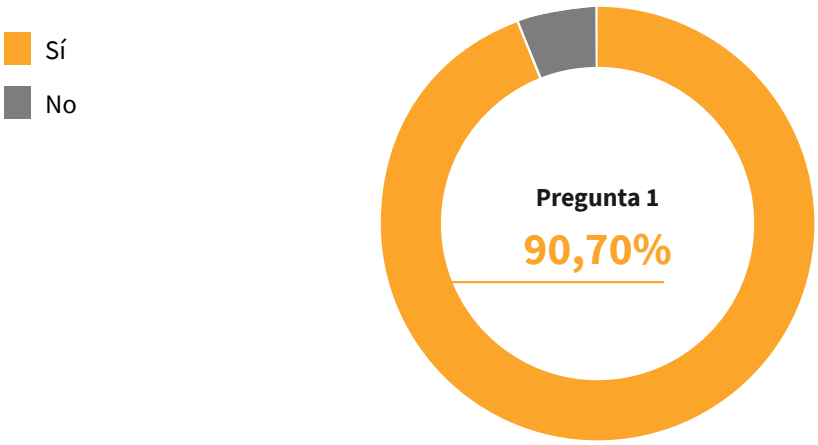
Encuestas de Calidad 2022			
Resumen general		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	5.901	605
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	5.924	582
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	6.081	425
Total de encuestas realizadas		**6.506**	

Análisis de respuestas		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	90,70%	9,30%
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	91,05%	8,95%
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	93,47%	6,53%
Total de encuestas realizadas		**100%**	
Promedio de satisfacción		**91,74%**	

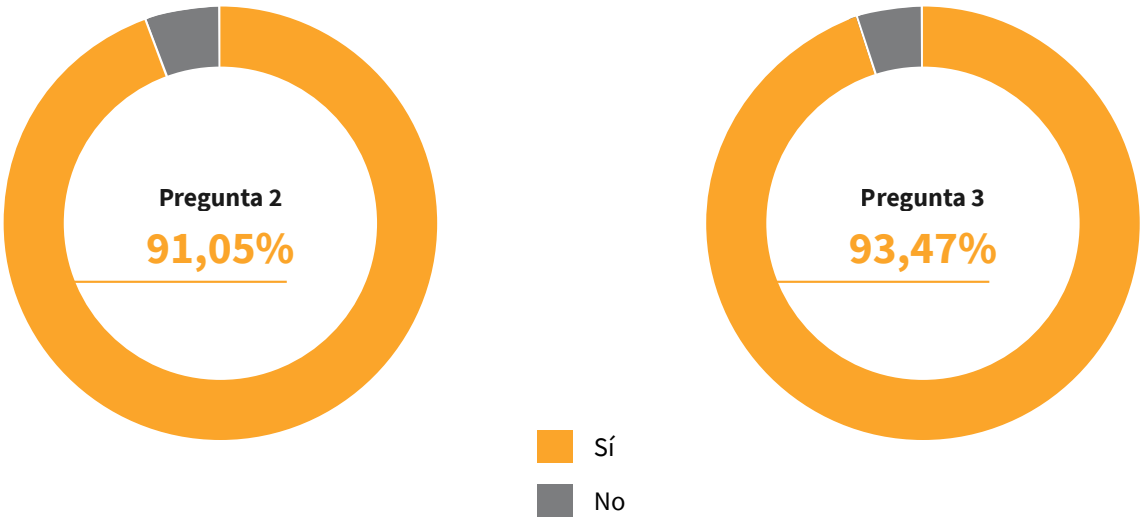
Encuestas de Calidad

Número Total 6.506

¿Está satisfecho con el contenido de la información recibida?



Encuestas de Calidad	
Número Total 6.506	
¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	¿Está satisfecho/a con la corrección en el trato por parte del operador?



Accesos a la sección de transparencia			
2020	2021	2022	% 2021-2022
138.264	166.290	127.549	-23,30%

Solicitudes de acceso a la información pública						
Año	Solicitudes	Concedidas	Inadmitidas[16]	Concedidas parcialmente	Denegadas	Desistidas
2022	177 [17]	70	72 [18]	12	5	13

[16] *Inadmitidas incluye devoluciones a la UIT Central. En 2021 fueron 22.*

[17] *5 solicitudes se encuentran todavía en trámite.*

[18] *Devueltas a UIT Central 23; finalizaciones anticipadas por acumulación y otras causas, 7.*

Reclamaciones ante el CTBG			
Año	Reclamaciones	Estimadas	Desestimadas
2022	6 [19]	0	4

[19] *2 reclamaciones están pendientes de resolución por parte del Consejo de Transparencia y Buen Gobierno.*

Registro de Delegados de Protección de Datos comunicados [20]		
Titularidad		Total notificados
Entidades Privadas		91.221
Entidades Públicas		9.129
	Administración General del Estado	182
	Comunidades Autónomas	433
	Entidades Locales	4.537
	Otras personas Jurídico-Públicas - Consejo General del Poder Judicial - Notarios - Colegios Profesionales - Universidades - Cámaras de Comercio - Comunidades Regantes	3.977
TOTAL		**100.350**

[20] *Durante 2022 se han atendido 1.059 consultas e incidencias relativas a la comunicación de los DPD*

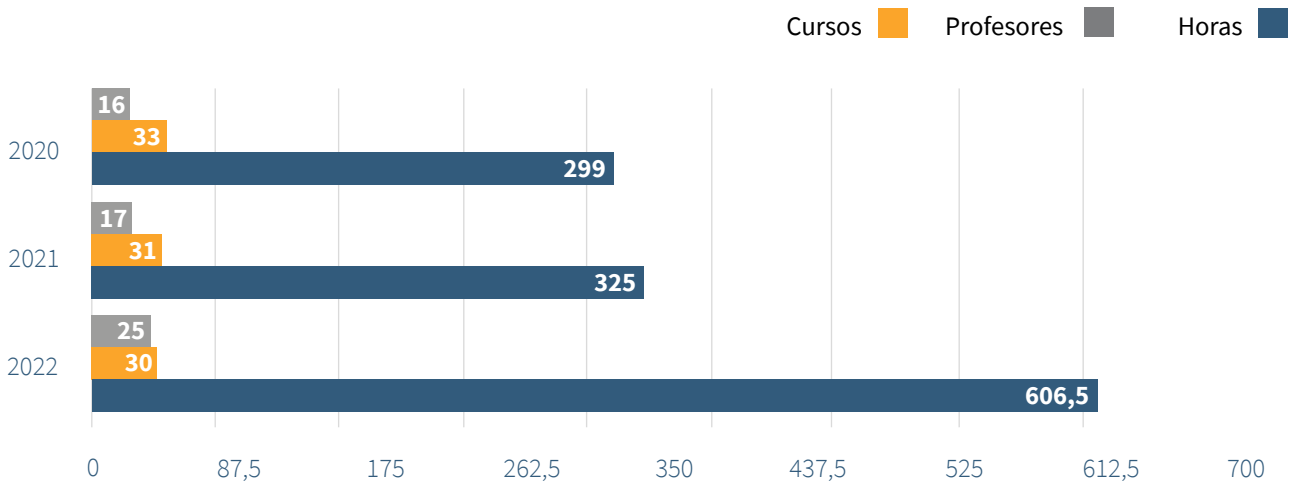
Transferencias Internacionales desde 2019		
	2022	Total acumulado
Autorizaciones de transferencias internacionales	-	1 (Art. 46.3.b RGPD)
Normas Corporativas Vinculantes (BCR) adoptadas por la AEPD	1	7
Normas Corporativas Vinculantes (BCR) en tramitación por la AEPD como autoridad líder	6	-
Normas Corporativas Vinculantes (BCR) en las que la AEPD ha participado como co-revisora	7	33

Esquema de Certificación de DPD (AEPD-DPD)			
	2020	2021	2022
Auditorías	9	12	4
Revisión de preguntas de examen	1.927	8.538	3.932
Elaboración de exámenes	61	95	72
Seguimiento de entidades de formación	68	164	136
Seguimiento de entidades de certificación	7	13	15
Reconocimiento de formación universitaria	0	1	1
DPD Certificados	200	175	138
Total DPD Certificados:			**927**

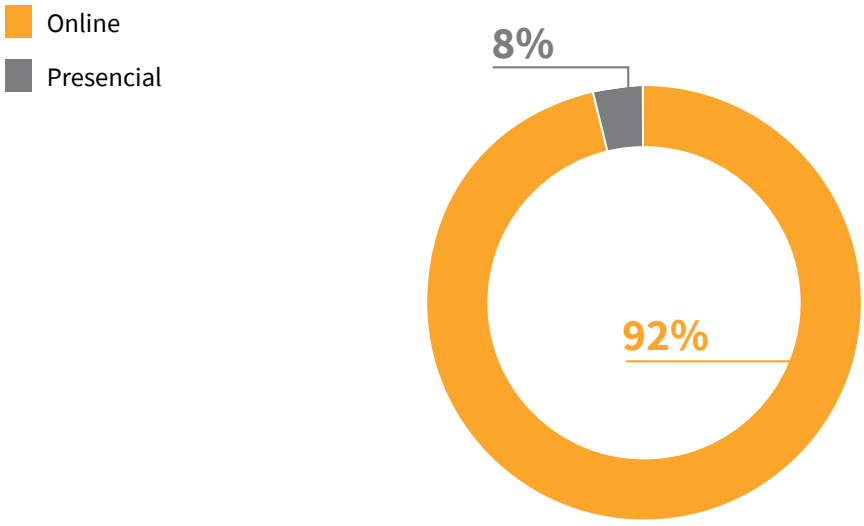
Formación [21,22]			
	2020	2021	2022
Cursos	16	17	25
Profesores	33	31	30
Horas	299	325	606,5

[21] *Coordinados por la Subdirección General de Promoción y Autorizaciones*

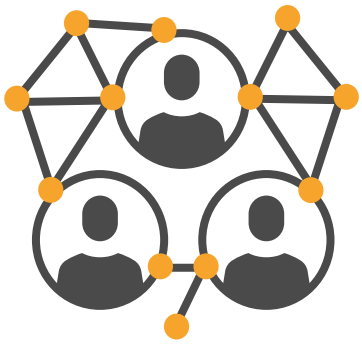
[22] *Media de alumnos por curso 40*



Formato del curso



Facilita RGPD [23]	
	2022
Accesos	56.586
Cuestionarios finalizados	21.563
Acumulados	**1.057.378**



[23] Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales.

Facilita EMPRENDE [24]	
	2022
Accesos	3.525
Cuestionarios finalizados	871
Acumulados	**15.954**

[24] Facilita EMPRENDE, herramienta para ayudar a los emprendedores y startups tecnológicas a cumplir con la normativa de protección de datos.

GESTIONA [25]			
Sección	Abierto	Finalizado	Acumulados
Evaluaciones de impacto en la privacidad (EIPD)	3.733	1.885	30.678
Análisis de riesgos	3.269	1.612	29.491

[25] Gestiona EIPD: Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos.

COMUNICA-Brecha RGPD [26]	
	2022
Accesos	4.830
Cuestionarios finalizados	690
Acumulados	**11.362**

[26] *Comunica-Brecha RGPD, recurso para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales.*

Evalúa-Riesgo RGPD [27]		
	2021	**2022**
Accesos	6.134	101.897
Acumulados		**108.031**

[27] *Evalúa_Riesgo RGPD: herramienta disponible en su versión web desde el 14 de septiembre de 2022, cuyo objetivo es ayudar a los responsables y encargados a identificar los factores de riesgo de los tratamientos de datos personales; hacer una primera evaluación no exhaustiva, del riesgo intrínseco, incluyendo la obligación de realizar una EIPD, y facilitando la gestión del riesgo residual al utilizar medidas y garantías para mitigar dicho riesgo.*

4. Secretaría General

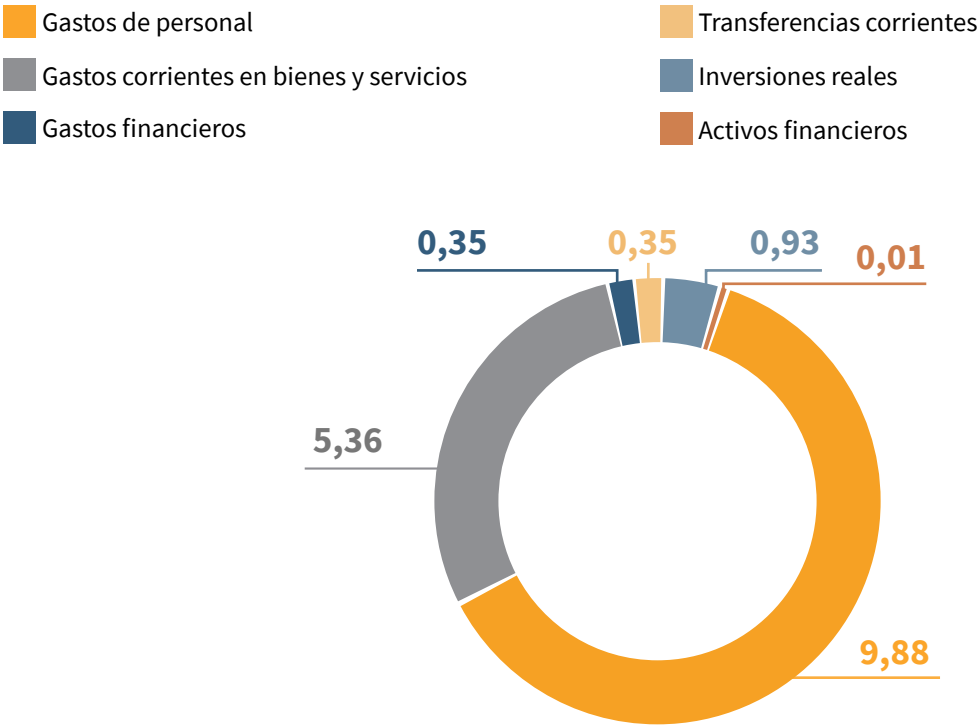
Evolución del presupuesto					
	Crédito Ejercicio				
	2020	2021	% INC 20/21	2022	% INC 21/22
Capítulo I	7.986.570	8.751.570	10	9.882.840	13
Capítulo II	4.956.060	5.235.310	6	5.359.840	2
Capítulo III	40.950	350.950	757	350.950	0
Capítulo IV	284.440	475.520	67	350.990	-26
Capítulo VI	937.860	928.350	-1	928.350	0
Capítulo VIII	22.800	20.800	-9	11.200	-46
TOTAL	**14.228.680**	**15.762.500**	**11**	**16.884.170**	**7**

2022			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	9.882.840,00	9.505.277,87	96,18%
Gastos corrientes en bienes y servicios	5.359.840,00	4.818.377,76	89,90%
Gastos financieros	350.950,00	160.954,37	45,86%
Transferencias corrientes	350.990,00	347.990,00	99,15%
Inversiones reales	928.350,00	669.939,18	72,16%
Activos financieros	11.200,00	6.629,14	59,19%
TOTAL	**16.884.170,00**	**15.509.168,32**	**91,86%**

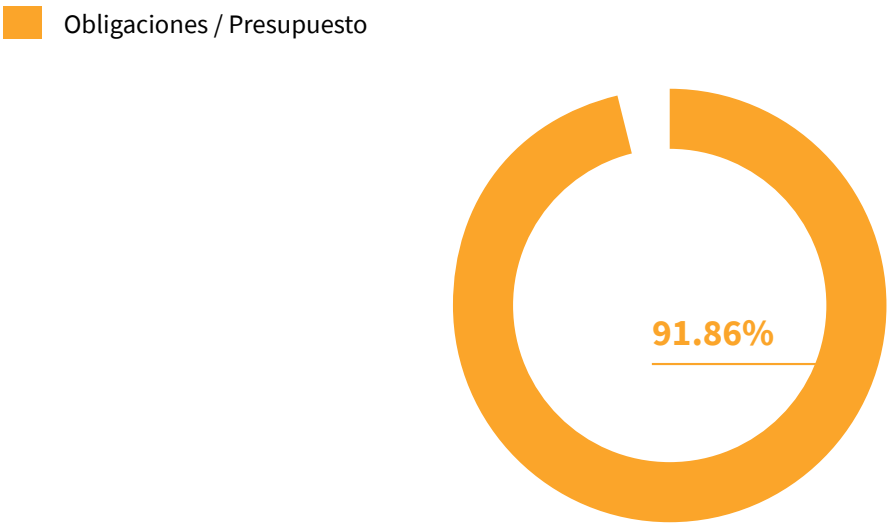
2021			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	8.967.328,00	8.284.068,81	92,38%
Gastos corrientes en bienes y servicios	5.211.088,34	4.881.792,69	93,68%
Gastos financieros	350.950,00	124.655,41	35,52%
Transferencias corrientes	350.983,66	344.983,66	98,29%
Inversiones reales	861.350,00	828.773,06	96,22%
Activos financieros	20.800,00	0	0,00%
TOTAL	**15.762.500,00**	**14.464.273,63**	**91,76%**

Diferencia 2021 - 2022		
	Presupuesto definitivo	Obligaciones reconocidas
Gastos de personal	915.512,00	1.221.209,06
Gastos corrientes en bienes y servicios	148.751,66	-63.414,93
Gastos financieros	0	36.298,96
Transferencias corrientes	6,34	3.006,34
Inversiones reales	67.000,00	-158.833,88
Activos financieros	-9.600,00	6.629,14
TOTAL	**1.121.670,00**	**1.044.894,69**

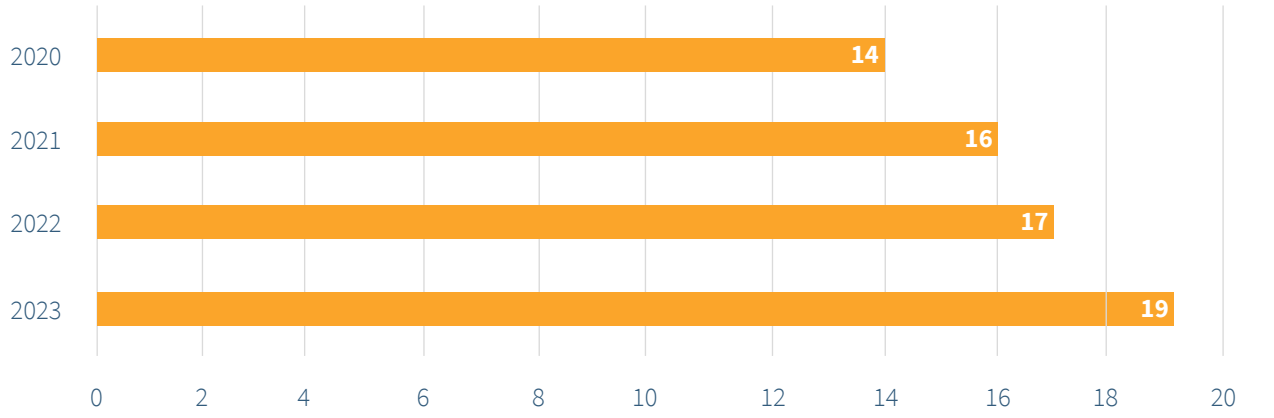
Distribución del presupuesto (millones de €)



Ejecución presupuestaria



Evolución del crédito presupuestario (millones de €)

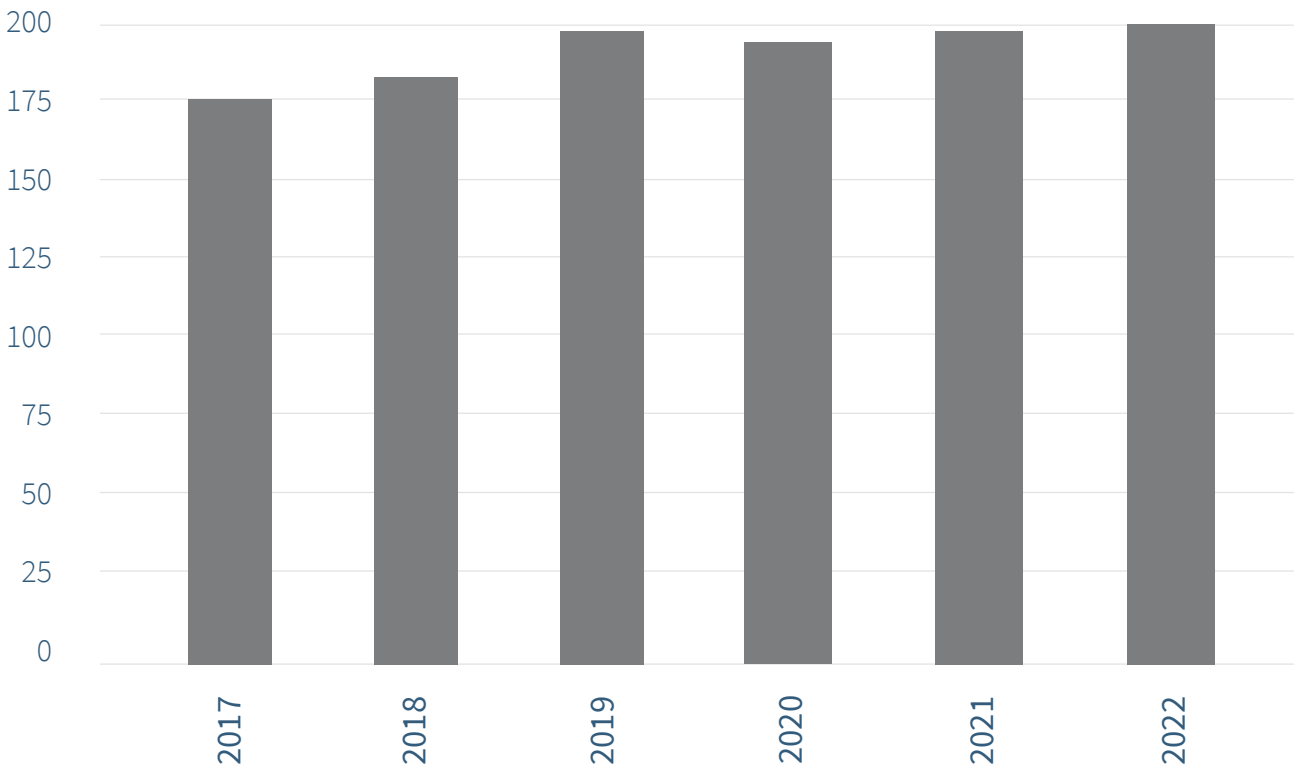


Gestión de recursos humanos a 31 de Diciembre 2022

	Dotación	Cubiertos
Funcionarios	207	175
Laborales	8	6
Laborales fuera de Convenio	2	2
Alto cargo	1	1
TOTAL	**218**	**184**

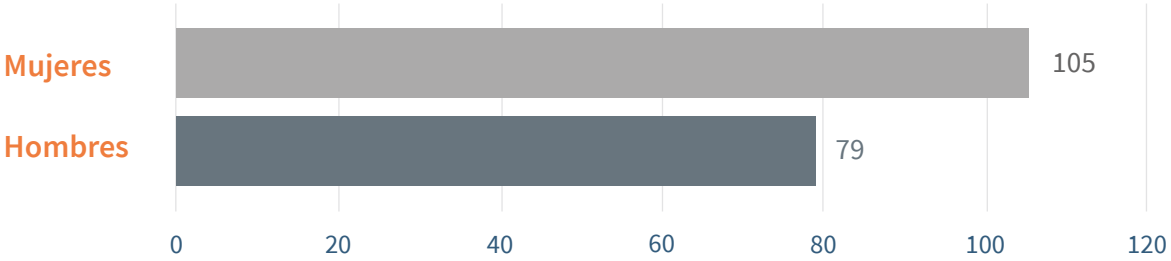
La diferencia entre el número total de dotaciones y la ocupación efectiva es debida a que dentro de las 207 plazas totales correspondientes a personal funcionario se incluyen los puestos reservados cuyos titulares se encuentran ocupando otro puesto, así como los puestos de niveles mínimos, 14 y 15, cuya cobertura ha sido imposible tras diferentes procesos de provisión convocados y que de hecho van a ser amortizadas en 2023.

Evolución RPT AEPD (2017-2022)



Año	Dotaciones (*)
2017	180
2018	186
2019	202
2020	202
2021	203
2022	217

(*) *Personal funcionario más personal laboral menos alto cargo.*



Antes de la aprobación del Plan de Igualdad de la AEPD, en abril de 2020, se partía de un 61,54 % de hombres frente a un 38,46 % de representación femenina en puestos de niveles 26 a 30. Este último porcentaje ha ascendido al 49,12 %.

Funcionarios												
Nivel	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	8	7	38	60	0	24	3	28	1	6	0	0

Grupo	A1	A2	B	C1	C2
Efectivos	58	62	1	33	22

5. Presencia internacional de la AEPD

Reunión	Fecha	Lugar
Sesiones Plenarias del Comité Europeo de Protección de Datos	18 de enero 1 de febrero 22 de febrero 14 de abril 6 de abril 4 de mayo 12 de mayo	Videoconferencia
	14 y 15 de junio	Bruselas (Bélgica)
	12 de julio 28 de julio	Videoconferencia
	12 y 13 de septiembre 10 de octubre	Bruselas (Bélgica)
	14 de noviembre 5 de diciembre	Videoconferencia
	13 y 14 de diciembre	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de datos

Reunión	Fecha	Lugar
Subgrupo de asesoramiento (Strategic advisory)	1 de abril 7 de junio 5 de septiembre 15 de septiembre 21 de octubre 14 de noviembre	Videoconferencia
Grupo de trabajo Cookie Banners	12 de enero 2 de febrero 8 de marzo 29 de marzo 13 de abril 11 de mayo 17 de junio 29 de septiembre 28 de octubre 12 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Medios Sociales Digitales (Social Media)	10 de febrero 31 de marzo	Videoconferencia
	5 de mayo	Bruselas (Bélgica)
	8 de septiembre 20 de octubre	Videoconferencia
	8 de diciembre	Bruselas (Bélgica)
Usuarios de sistemas de información del CEPD (IT Users)	29 de marzo 25 de julio	Videoconferencia
	20 de septiembre 1 de diciembre	Bruselas (Bélgica)
Cooperación	26 de enero 15 de febrero 24 de febrero 22 de marzo 26 de abril 30 de mayo 22 de junio 20 de julio 21 de septiembre 21 de octubre 23 de noviembre 15 de diciembre	Videoconferencia
Asuntos financieros	9 de febrero 3 de marzo 18 de marzo 12 de abril 19 de mayo 4 de julio 9 y 13 de septiembre 19 de septiembre 28 de septiembre 22 de noviembre 12 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Transferencias internacionales	25 y 26 de enero 15 y 16 de febrero 15 y 16 de marzo 20 de abril	Videoconferencia
	17 y 18 de mayo	Cavtat (Croacia)
	31 de mayo 7 de junio 19 de julio	Videoconferencia
	8 de septiembre 18 y 19 de octubre	Bruselas (Bélgica)
	8 de noviembre 6 y 7 de diciembre	Videoconferencia
Grupo de trabajo Multas	9 de marzo 25 de marzo 10 de junio 24 de noviembre	Videoconferencia
Grupo de trabajo sobre las 101 denuncias presentadas tras la sentencia Schrems II del TJUE	11 de enero 9 de febrero 23 de marzo 20 de abril 20 de mayo 22 de julio 5 de octubre 3 de noviembre 23 de noviembre	Videoconferencia
Fronteras, viajeros y aplicación legislativa (BTLE)	11 de enero 27 de enero 3 de marzo 7 de abril	Videoconferencia
	19 de mayo 7 de julio	Bruselas (Bélgica)
	22 de septiembre 27 de octubre 24 de noviembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Disposiciones clave (Key Provisions)	9 de marzo 31 de mayo 5 de julio	Videoconferencia
	27 de septiembre	Bruselas (Bélgica)
	10 de noviembre 9 de diciembre	Videoconferencia
Supervisión del cumplimiento (Enforcement)	25 de enero 23 de marzo 24 y 25 de mayo 8 de junio 20 de junio 23 de junio 30 de junio 5 de julio 18 de julio 19 de julio 20 de septiembre 12 y 13 de octubre 24 de octubre 26 de octubre 4 de noviembre 7 de noviembre 11 de noviembre 15 y 16 de noviembre 17 de noviembre 21 y 22 de noviembre	Videoconferencia
Tecnología	20 de enero 16 y 17 de febrero 16 de marzo 7 de abril 5 de mayo 2 de junio 6 y 7 de julio 11 de julio 15 de julio	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Tecnología	7 de septiembre	Bruselas (Bélgica)
	19 y 20 de octubre 9 de noviembre	Videoconferencia
	7 de diciembre	Bruselas (Bélgica)
Cumplimiento, Gobierno electrónico y Salud (Compliance, E-goverment & Health)	17 y 19 de enero 25 de febrero 28 de marzo 8 de abril 21 de abril 17 de mayo 1 de junio 10 de junio 20 de junio	Videoconferencia
	29 y 30 de junio 13 de julio 14 de septiembre 13 y 14 de octubre	Bruselas (Bélgica)
	10 de noviembre 21 de noviembre 6 de diciembre 19 y 20 de diciembre	Videoconferencia

Control de Agencias y Grandes Sistemas de Información UE		
Reunión	**Fecha**	**Lugar**
Grupo de Supervisión Coordinada CSC	6 julio 30 noviembre	Bruselas (Bélgica)
Grupo de Supervisión Coordinada del SIS II	21 de noviembre	
Grupo de Supervisión Coordinada del VIS + EURODAC	22 noviembre	
Grupo de Supervisión Coordinada de EUROPOL	30 de noviembre	

Control de Agencias y Grandes Sistemas de Información UE		
Reunión	**Fecha**	**Lugar**
Evaluación Schengen	13 al 18 de marzo	Luxemburgo
	13 al 17 de junio	Estocolmo (Suecia)

Consejo de Europa		
Reunión	**Fecha**	**Lugar**
Comité Convención 108 – Mesa	23 al 25 de marzo	Videoconferencia
Comité de Inteligencia Artificial	4 al 6 de abril	
Comité Convención 108 – Mesa	21 y 22 de septiembre	Estrasburgo (Francia)
Comité de Inteligencia Artificial	21 al 23 de septiembre	
Comité Convención 108 - Plenario	16 al 18 de noviembre	
	15 y 16 de diciembre	

Otras reuniones		
Reunión	**Fecha**	**Lugar**
Mobile World Congress	28 de febrero al 2 de marzo	Barcelona
Comissioner's Summit	26 al 28 de abril	Viena (Austria)
Coloquio sobre el acceso a los datos	20 al 22 de abril	Paris (Francia)
Grupo de Berlín	31 de mayo al 2 de junio	Tel Aviv (Israel)
Spring Conference	19 y 20 de mayo	Cavtat (Croacia)
Conferencia Anual CPDP	23 al 25 de mayo	Bruselas (Bélgica)
Annual Privacy Forum	23 y 24 de junio	Varsovia (Polonia)

Otras reuniones		
Reunión	**Fecha**	**Lugar**
Parlamento Europeo – Comité LIBE	11 de octubre	Videoconferencia
Global Privacy Assembly	25 – 27 de octubre	Estambul (Turquía)
Grupo de Berlín	28 – 30 de noviembre	Londres (Reino Unido)
"International Intelligence Oversight Forum" (IIOF)	14 y 15 de noviembre	Estrasburgo (Francia)
Conferencia “Protección de datos y justicia penal”	29 de noviembre	Bruselas (Bélgica)

Reuniones RIPD	
Reunión	**Número de encuentros**
Reunión con el Secretario Ejecutivo de la Corte Interamericana de Derechos Humanos	1
Reunión con AGETIC (Bolivia)	2
Foro de Sociedad Civil (FSC)	2
APD Panamá	1
Colaboración proyecto financiado por la UE	3
AIPyC (Asociación Iberoamericana de Protección de Datos y Ciberseguridad)	1
INAI México	2
BID (Banco Interamericano de Desarrollo)	1
AECID (Agencia Española de Cooperación Internacional para el Desarrollo)	8
APD Colombia	1

Reuniones RIPD	
Reunión	**Número de encuentros**
ALAP (Asociación de Profesionales de Privacidad de América Latina) y APEP (Asociación Profesional Española de Privacidad)	1
Defensoría Pueblo Argentina	1
Costa Rica	1
Sula Batsu y ADC	1
Grupo de Trabajo de la RIPD para las relaciones con la industria de internet	1
SEGIB (Secretaria de Estado para Iberoamérica y el Caribe y el Español en el Mundo)	1

www.aepd.es