MEMORIA ANUAL

2024

agencia española protección datos

prólogo

Es un honor para mí, como nuevo presidente de la Agencia Española de Protección de Datos (AEPD), presentar el trabajo desarrollado por las diferentes unidades del organismo durante el año 2024. La nueva dirección hemos tenido la suerte de heredar una Agencia enérgica, proactiva y con muchas ganas de afrontar el futuro.

Podría señalar un número considerable de objetivos alcanzados durante el pasado ejercicio, si bien sólo me detendré en algunos de ellos, ya que las cifras más relevantes, así como todas las iniciativas, proyectos y demás acciones que la AEPD ha desarrollado durante el año 2024, pueden consultarse en el contenido de esta memoria.

Como es sabido y durante estos últimos tiempos, la **protección de las personas menores de edad en el ámbito digital**, el tiempo que utilizan dispositivos móviles, los servicios de internet a los que acceden, así como las consecuencias a nivel sanitario, afectivo y de desarrollo que experimentan ha sido una de las grandes preocupaciones de la Agencia. Es por ello que en 2024 se desplegaron diferentes tipos de iniciativas, que incluyeron el desarrollo de herramientas tecnológicas y acciones de concienciación, sensibilización y formación, cuyo objetivo primordial consistía en garantizar los derechos de la infancia y de la adolescencia y el ejercicio de las potestades de investigación y sanción.

El desarrollo del **sistema de verificación de edad**, para proteger a las personas menores de edad ante el acceso a contenidos de personas adultas en Internet, acompañado de un decálogo de principios, ha permitido establecer un marco de actuación que ha concluido con la aprobación de un Dictamen, por parte del Comité Europeo de Protección de Datos, sobre la determinación de la edad para el uso de servicios on line que requieren de una edad mínima para poder acceder a ellos.

A nivel nacional, la Agencia viene trabajando, desde hace una década, en el ámbito de la **protección de las personas menores de edad en el mundo digital**. En concreto, el año pasado ha formado parte del Comité de personas expertas, cuya creación fue aprobada por el Consejo de Ministros a principios de 2024, bajo la coordinación del Ministerio de Juventud e Infancia con el objetivo de proteger a los y las menores en el mundo digital. Los trabajos de este Comité concluyeron con la propuesta de 107 medidas para crear entornos digitales seguros y permitieron al gobierno la aprobación del Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales.

Un segundo aspecto que ha ocupado y que sin duda va a ocupar gran parte del trabajo de la Agencia en los próximos años, es todo lo relativo al procesamiento de datos personales con **inteligencia artificial (IA)** así como los sistemas de alto riesgo. Sin duda, el Reglamento de Inteligencia Artificial (RIA), publicado en el Diario Oficial de la Unión Europea (DOUE) en julio de 2024, marca un hito importante en la regulación de la IA en el mercado único europeo y afectará de forma directa a las competencias que se atribuirán a las autoridades nacionales en materia de protección de datos. La Agencia es y va a ser la autoridad de control esencial respecto de todo tratamiento de datos personales con IA, además de las diversas responsabilidades y atribuciones debido al desarrollo del RIA y otras normas europeas y españolas.

En otro orden de cosas, una de las materias sobre las que la AEPD se ha implicado en los últimos años ha sido la relativa a los **espacios de compartición de datos**. La disponibilidad de datos de alta calidad supone un avance muy relevante para la toma de decisiones y la personalización de los servicios en diferentes ámbitos de nuestra vida, si bien el acceso masivo a datos plantea retos significativos en términos de privacidad y protección de los derechos de las personas. Se trata de un ámbito en el que las atribuciones de la Agencia también son crecientes, como su implicación en la gobernanza con otras autoridades y entidades en el despliegue de los espacios de datos, con el caso de salud como ariete y reto inicial para todos. **La posición de la Agencia es clara**: evitar en lo posible que la protección de datos sea una barrera a una política que es esencial en la Unión Europea para el desarrollo económico, investigador y social, pero, obviamente, garantizando el cumplimiento de la legislación de protección de datos y una cultura de responsabilidad y transparencia, asegurando que la confianza de la ciudadanía en el uso de sus datos no se vea comprometida.

Las posibilidades del uso de datos a gran escala son enormes y con aplicación directa a la inteligencia artificial. De hecho, la AEPD tiene previsto seguir reforzando esta área de trabajo para poder generar conocimiento, mediante el abordaje de los retos de **una IA ética** desarrollada e implementada teniendo en cuenta las necesidades de la ciudadanía en general y de los colectivos vulnerables en particular. Y también reforzando el conocimiento interno del personal de la AEPD y analizando aspectos relevantes en los escenarios de acceso a cantidades masivas de datos, en particular sobre datos sanitarios en los entornos de procesamiento seguro que recoge el Reglamento del Espacio Europeo de Datos Sanitario.

Entre las iniciativas más innovadoras y relevantes en las que la Agencia ha venido trabajando en los últimos años, cabe destacar la elaboración de propuestas para garantizar el tratamiento de los **neurodatos** en el marco de la normativa reguladora del derecho fundamental

a la protección de datos personales, ante la ausencia de una regulación específica sobre esta materia. Los neurodatos pueden revelar información íntima sobre el estado de salud, pensamientos o emociones y pueden identificar a una persona de manera única. Todo ello representa un desafío significativo para la protección de datos debido a la naturaleza personal y, en ocasiones, extremadamente sensible de tal información.

Respecto a los avances en este ámbito y la gestión de los desafíos que plantea la **neurotecnología**, la AEPD ha venido colaborando con el Supervisor Europeo de Protección de Datos (EDPS) analizando las implicaciones del tratamiento de neurodatos y ofreciendo recomendaciones concretas, para fomentar un desarrollo tecnológico que respete y proteja los derechos fundamentales en el entorno digital. Asimismo, en el ámbito iberoamericano y con motivo de la celebración del XX aniversario de la Red Iberoamericana de Protección de Datos, la AEPD participó en la Declaración sobre neurodatos, aprobada por el Comité Jurídico Interamericano de la OEA. Sin duda, ya ha pasado el tiempo de las declaraciones de derechos y principios en este ámbito, es momento ya de ir perfilando lo que deberían ser las garantías y salvaguardas necesarias, en su caso, a través de los correspondientes desarrollos legislativos.

Otra de las prioridades de la AEPD en un futuro próximo será la **identidad digital**, materia que se encuentra en Europa en un momento de transformación significativa tras la publicación del reglamento eIDAS2, que persigue proporcionar a todos los ciudadanos y residentes en la UE una forma armonizada, segura y confiable de identificarse y acceder a servicios tanto públicos como privados. Una identidad digital bien diseñada e implementada debe permitir a la ciudadanía un mayor control sobre sus datos personales, ya pueden decidir qué información comparten y con quién. Está previsto que la Agencia asuma nuevas responsabilidades que deriven de la aplicación del nuevo reglamento eIDAS2, en continua colaboración con el CEPD y con ENISA.

A **nivel internacional**, es particularmente destacable cómo la reciente adopción del paquete legislativo digital ha impactado considerablemente sobre el RGPD y la actividad del Comité Europeo de Protección de Datos (EDPB).

Durante 2024, en el seno del EDPB se ha trabajado en diferentes proyectos, como el desarrollo de unos *Principios europeos de alto nivel para sistemas de verificación de edad*, basados en el decálogo que elaboró la AEPD en 2023; el desarrollo de las *Directrices sobre blockchain*; la elaboración de las *Directrices sobre acceso biométrico a servicios físicos* como entornos laborales, gimnasios o estadios; el *Dictamen sobre el consentimiento válido en el contexto de los modelos de consentimiento o pago aplicados por servicios digitales que no son grandes plataformas en línea*, típicamente periódicos online.

En relación con el tratamiento de **datos biométricos**, se detalla en la memoria la particular actividad de la AEPD al respecto y en coordinación con la autoridad de Baviera. Como es sabido, lo relativo a la naturaleza y régimen jurídico del tratamiento de los datos biométricos es un ámbito de cierta conflictividad respecto del que hay que estar muy pendiente y a la vez proactivos respecto de la valoración última coordinada en el EDPB que se llevará a lo largo de 2025. Esta visión común y coordinada y debe llevar a evitar las diferencias y asimetrías que se observan en los diferentes Estados de la Unión.

La inflación legislativa europea vivida en los últimos años en materia de servicios digitales, datos e inteligencia artificial, ha supuesto la adopción de numerosas normas que tienen un importante impacto sobre la protección de datos personales. Todo ello supondrá una importante carga de trabajo y de nuevas atribuciones que esta Agencia deberá afrontar a corto y medio plazo, lo que debería ir acompañada de la posibilidad de contar con una dotación presupuestaria y un incremento de personal acorde con la cantidad y calidad de trabajo que le corresponderá asumir, tal y como ha determinado el Consejo de la Unión Europea, en su propuesta de Decisión de Ejecución de 2024, a fin de poder desempeñar con eficacia las funciones que le atribuye el acervo comunitario.

No quisiéramos finalizar este prólogo sin agradecer la dedicación y el esfuerzo diario de todos los equipos que constituyen la Agencia y que hacen posible detallar el ingente trabajo desarrollado que se expresa con minucioso detalle en las páginas siguientes. Y, obviamente, a la anterior directora de la Agencia que dejó el puesto justo a finales de 2024.

Es un orgullo integrarse y trabajar junto a un equipo tan comprometido, cohesionado y siempre dispuesto a asumir nuevos retos, manteniendo el ritmo diario para mantener a esta Agencia en la vanguardia de la protección de un derecho fundamental que se demuestra cada vez más importante en la sociedad digital en la que nos encontramos.

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos

Francisco Pérez Bes
Adjunto de la Agencia Española de Protección de Datos

índice

La agencia en cifras

1. Principales hitos de 2024

LA PROTECCIÓN DEL MENOR

En la Memoria del año 2023 se destacó, como una de las principales preocupaciones de la Agencia, el acceso a los dispositivos móviles por parte de los y las menores en el entorno digital, así como el tiempo de uso y los servicios de Internet a los que acceden, considerando los graves efectos perjudiciales para su salud (física, mental, psicosocial, sexual); su neurodesarrollo; su aprendizaje; sus relaciones familiares y sociales o a la monetización de sus datos. Por este motivo, las iniciativas adoptadas para dar respuesta a esta situación ocuparon un lugar destacado en la agenda de este organismo durante todo el año 2024.

La AEPD puso en marcha diversas iniciativas y líneas de trabajo específicas para la protección del menor en el mundo digital. Estas acciones se centraron en varios aspectos clave, desde la concienciación y la educación hasta el desarrollo de herramientas y recursos adaptados a este grupo vulnerable.

A principios de 2024, la Agencia diseñó una **nueva estrategia reforzada**, constituida por 10 actuaciones prioritarias y 35 medidas, agrupadas en tres ejes estratégicos: la colaboración regulatoria, el refuerzo para garantizar los derechos de la infancia y la adolescencia y el ejercicio de las potestades de investigación y sanción, además de incluir dos grandes bloques centrados en la educación, y la salud y el bienestar digital.

En relación con los proyectos ya iniciados, la AEPD continuó impulsando las reuniones del Grupo de Trabajo, lanzado en 2019, para la protección de los menores en el mundo digital "Menores, salud digital y privacidad", con la finalidad de abordar aquellas situaciones del uso de las TIC que afectan a su privacidad, bienestar y salud digital, en definitiva, a su desarrollo integral como personas, pues la protección de sus datos y de su privacidad es proteger su desarrollo.

En el marco de la labor de concienciación que le corresponde, la Agencia difundió, junto a la Fundación Atresmedia, la campaña **"No a la barra libre digital"**, para alertar sobre los peligros del acceso de los y las menores a contenidos inadecuados a través del móvil y promover el acompañamiento en el uso de la tecnología en la infancia y adolescencia. Esta campaña recomendaba a las familias que retrasasen la entrega del móvil a sus hijos e hijas y los acompañasen en su interacción con el mundo digital, evitando así que accedieran a contenidos inapropiados y perjudiciales para su desarrollo, como contenidos pornográficos o violentos.

Otra de las acciones de sensibilización que divulgó la Agencia en 2024 llevó el título **"Hay más riesgos en Internet que en la vida real"**, relacionada con el acceso online por los y las menores a contenidos para personas adultas, en especial a la pornografía que, según los estudios e informes de organizaciones especializadas señalan que se viene produciendo en torno a los 9 años, una edad en la que su desarrollo cognitivo no les permite entender lo que están viendo, pues su personalidad no está formada y genera importantes desórdenes en la concepción de las relaciones sexuales y del rol de la mujer.

La AEPD continuó actualizando los contenidos de la sección específica de su página web dedicada al tratamiento de datos personales de menores y al ámbito educativo, del mismo modo que mantuvo el canal de atención y consulta específico para menores de edad, permitiéndoles tanto a ellos y ellas como a sus representantes, plantear dudas y obtener orientación sobre cuestiones relacionadas con la protección de sus datos en el entorno digital.

También, durante 2024, la AEPD promovió el **Pacto Digital para la Protección de las Personas**, una iniciativa que busca involucrar a diferentes actores en la protección de los derechos de la ciudadanía en el entorno digital.

Dentro de este mismo ámbito de protección de menores en el entorno digital, la Agencia, además de ofrecer recomendaciones para las familias a

través del **Plan Digital Familiar**, proporcionando pautas y consejos prácticos para ayudar a los padres y madres a proteger a sus hijos e hijas en el entorno digital, también presentó dos informes sobre la influencia de los patrones adictivos en Internet, especialmente en menores de edad, y cómo afectan a los derechos fundamentales. Ambos con el objetivo de concienciar sobre los posibles daños a la integridad física y mental que puede causar la exposición prolongada a estos patrones basados en sus datos personales.

Una de las iniciativas más pioneras de la AEPD en los últimos años y que le permitió ser galardonada con varios premios fue la relacionada con los sistemas de **verificación de la edad**. Esta propuesta fue presentada a finales de 2023 y experimentó un notable desarrollo tanto a nivel nacional como internacional, captando un interés relevante y siendo reconocida por su innovación y relevancia en el ámbito de la protección de la privacidad y la seguridad en línea. En 2024, como resultado de su impacto y acogida, la iniciativa recibió dos premios en la Global Privacy Assembly, destacando su liderazgo a nivel mundial en el campo de la protección de datos y otros cuatro premios a nivel nacional, lo que subrayó la importancia de la iniciativa en el ámbito local y su contribución a la mejora de la seguridad digital en España.

A lo largo de 2024, la iniciativa dio lugar a numerosas colaboraciones estratégicas que permitieron su expansión y desarrollo en diversos contextos. Una de las más destacadas fue la creación del "Grupo de Trabajo para Determinar las Funcionalidades del Sistema de Control en el Acceso a Contenidos para Personas Adultas", impulsado por el Ministerio de Transformación Digital y Políticas Públicas. Este grupo tuvo como objetivo principal apoyar el desarrollo de una herramienta de verificación de edad, diseñada para garantizar un acceso seguro a contenidos en línea, particularmente para proteger a los y las menores de edad de contenidos inapropiados. Esta herramienta tomó como referencia la **cartera digital europea**, una solución innovadora que busca proporcionar una **verificación de edad robusta y respetuosa** con la privacidad de los usuarios. La AEPD juega un papel crucial en este grupo de trabajo, colaborando activamente en la formulación y el diseño de las funcionalidades del sistema, lo que refuerza su liderazgo en la promoción de la protección de los datos personales y la seguridad digital en el entorno online.

Hay que destacar que, en una reunión celebrada en el plenario del Comité Europeo de Protección de Datos (CEPD) se adoptó un Dictamen sobre la determinación de la edad para el uso de servicios online que requieren de una edad mínima para poder acceder a ellos.

En el contexto de la protección de los menores en Internet, se llevaron a cabo dos iniciativas fundamentales que destacaron por su carácter pionero y su relevancia en la creación de un entorno digital más seguro para los niños/niñas y adolescentes. La primera de ellas fue la publicación de un **Informe sobre la influencia de los patrones adictivos en Internet**, que aborda de manera profunda los efectos de los mecanismos y patrones diseñados para fomentar el uso continuo de Internet, en particular en lo que respecta a los y las menores de edad. Este informe examina cómo las plataformas digitales, mediante algoritmos y diseños de interfaces, pueden generar conductas adictivas que impactan negativamente en el bienestar de los y las menores, afectando tanto su desarrollo emocional como psicológico.

La segunda acción relevante fue la elaboración de una **Nota Técnica titulada "Internet seguro por defecto para la infancia y el papel de la verificación de edad"**. Esta nota se centra en la necesidad de establecer medidas tecnológicas y legales que garanticen que los servicios y plataformas digitales ofrezcan una experiencia de navegación segura por defecto para los y las menores, reduciendo al mínimo los riesgos asociados al acceso a contenidos inapropiados o peligrosos. Además, subraya la importancia de la verificación de edad como una herramienta clave para proteger la privacidad y la seguridad de los niños/niñas y adolescentes en línea, asegurando que sólo puedan acceder a servicios adecuados a su edad y que se respeten sus derechos en el entorno digital.

En el ámbito de las acciones de asesoramiento y el compromiso de la AEPD con la protección del menor, se colaboró con el Grupo Técnico de verificación de edad del Ministerio de Transformación Digital y Políticas Públicas y con el Comité de Expertos para la generación de un "entorno digital seguro para la juventud y la infancia".

En línea con todo lo anterior, no podemos olvidar que en el ámbito educativo es frecuente el uso de teléfonos inteligentes o tabletas, a menudo propiedad del alumnado o sus familias, y que

estos dispositivos pueden recopilar mucha información y tratarla con distintos propósitos más allá de la mera función educativa. Del mismo modo, los tratamientos de datos generados pueden afectar gravemente a los derechos y libertades del alumnado y a su desarrollo integral.

Conscientes de todo ello, la Agencia elaboró en 2024 una serie de **orientaciones sobre las obligaciones y responsabilidades por el uso de dispositivos móviles en los centros educativos**, dirigidas a las administraciones educativas, equipos directivos de centros escolares, docentes y familias, alertando de que, si un centro docente requiere al alumnado su dispositivo personal para una actividad pedagógica, podría incurrir en responsabilidad si se producen infracciones de la normativa. La AEPD desaconsejó su uso en los centros educativos si el fin pedagógico pretendido podía conseguirse a través de otro recurso más idóneo.

INTELIGENCIA ARTIFICIAL

Un ámbito que va a pasar a ser el centro de interés y de actuación de la Agencia en el futuro es el desarrollo de la inteligencia artificial (IA) y el análisis de su impacto en la protección de datos.

El **Reglamento de Inteligencia Artificial (RIA)**, publicado en el Diario Oficial de la Unión Europea (DOUE) en julio de 2024, marcó un hito importante en la regulación de la IA en el mercado único europeo. Este reglamento establece un marco normativo para el desarrollo, comercialización y uso de sistemas de IA, con un enfoque basado en el análisis de riesgos y, por tanto, alineado con la interpretación que el propio RGPD hace de los posibles impactos que las tecnologías pueden tener sobre los derechos y libertades de las personas físicas.

En 2024, la Agencia intensificó sus esfuerzos a través de la publicación de artículos en su blog, la creación de nuevas guías y la actualización de las existentes. Además, la AEPD lidera el **"Espacio de estudio sobre inteligencia artificial"**, un grupo de trabajo que reúne a personas expertas de diversas áreas, como la ingeniería informática, la filosofía y la ética, la investigación y la consultoría para analizar y discutir los retos y oportunidades de la IA. Entre las iniciativas de este Espacio de Estudio destaca la creación de un "Mapa de referencia para tratamientos que incluyen Inteligencia Artificial", dando paso a analizar las implicaciones de los nuevos escenarios de compartición y acceso masivo a datos.

Asimismo, la Agencia participó activamente en el Comité Europeo de Protección de Datos (EDPB) con la elaboración de guías sobre la IA, destacando su participación como coautora de la guía que analiza la relación entre el RIA y el RGPD. También colaboró con el EDPS en la elaboración de una nota técnica titulada "**10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)**". Además, para 2025, ha propuesto liderar el subgrupo sobre transparencia y participar en el de notificación de incidentes.

Al igual que la IA, van a ser de obligatoria referencia para la Agencia todas las cuestiones relacionadas con los **espacios de datos**. La disponibilidad de datos de alta calidad se constituye en un elemento clave para el entrenamiento de modelos de IA y su uso tiene el potencial de ser un factor de ayuda a la hora de mejorar la toma de decisiones y la personalización de servicios. Sin embargo, el acceso masivo a datos plantea retos significativos en términos de privacidad y protección de los derechos de las personas. En este contexto, los datos sanitarios, debido a su naturaleza especialmente sensible y otros tipos de datos provenientes de espacios de datos sectoriales, cobran especial relevancia por su sensibilidad y posible impacto sobre nuestra sociedad. La reutilización de datos para fines distintos a aquellos para los que fueron recolectados originalmente es y será, un eje fundamental en la construcción de espacios de datos de calidad.

La Agencia va a colaborar con otras autoridades y entidades y apostar en lo posible por facilitar el uso de datos para finalidades de interés público por sujetos públicos y privados, apostando por allanar el uso de datos para la investigación e innovación, obviamente con cumplimiento normativo y protección de datos.

BLOCKCHAIN

Dentro del marco de la promoción de las medidas de protección de datos desde el diseño, entre las iniciativas más destacables en el sector tecnológico cabe señalar la realización de una prueba de concepto sobre Blockchain y el RGPD.

La tecnología Blockchain ofrece la posibilidad de crear infraestructuras para el almacenamiento e intercambio de información de forma distribuida y descentralizada. Estas infraestructuras, adaptadas a objetivos específicos y complementadas con sistemas y aplicaciones adicionales, pueden ser utilizadas por diversos tratamientos, incluso compartiendo la misma infraestructura. La gestión de la infraestructura Blockchain también puede implicar tratamientos específicos de datos, si bien debe asegurar que el cumplimiento de los principios, derechos y obligaciones establecidos por el RGPD no se vea comprometido por la elección de una tecnología concreta. En este mismo sentido se ha manifestado el Comité Europeo de Protección de Datos.

Por ello, es imperativo para los responsables, encargados y desarrolladores conocer las posibilidades y limitaciones de los componentes que seleccionan para construir productos, servicios y tratamientos. Este conocimiento ha de partir de la evidencia objetiva obtenida a través de la documentación, certificación y/o auditoría de éstos, siendo clave el cuidado de la terminología utilizada, ya que en ocasiones generan confusión algunos conceptos y sus implicaciones, pudiendo generar equívocos sobre la realidad tecnológica.

NEURODATA

Uno de los proyectos que la AEPD viene desarrollando como iniciativa más innovadora y relevante consiste en desarrollar propuestas para garantizar el tratamiento de los neurodatos en el marco de la normativa reguladora del derecho fundamental a la protección de datos personales, ante la ausencia de una regulación específica sobre esta materia. Para el futuro, sin duda, se va a apostar por ir más allá de declaraciones genéricas o reconocimiento de nuevos derechos. Es momento ya de valorar posibles regulaciones o interpretaciones concretas que sirvan para garantizar la privacidad y la protección de datos y los derechos dimanantes de manera efectiva.

Los neurodatos pueden revelar información íntima sobre el estado de salud, pensamientos o emociones y pueden identificar a una persona de manera única. Todo ello representa un desafío significativo para la protección de datos debido a la naturaleza personal, y en ocasiones extremadamente sensible de los neurodatos.

Respecto a los avances en este ámbito y la comprensión y gestión de los desafíos que plantea la neurotecnología, destaca la colaboración de la AEPD con el EDPS en el documento titulado "**TechDispatch: Neurodatos**", donde se han analizado las implicaciones del tratamiento de neurodatos y se han ofrecido recomendaciones concretas, fomentando un desarrollo tecnológico que respete y proteja los derechos fundamentales en el entorno digital.

En esta línea de trabajo, durante la sesión del encuentro de la Red Iberoamericana de Protección de Datos (REDIPD) celebrada con motivo de su XX aniversario, la AEPD participó en la **Declaración sobre neurodatos** de la REDIPD aprobada por el Comité Jurídico Interamericano de la OEA. En dicha Declaración, se vino a subrayar que, si bien en el ámbito sanitario existe un marco jurídico específico que incorpora garantías adecuadas para los tratamientos de neurodatos, en otros ámbitos con tratamientos que conllevan fines distintos de los de salud, en los que existe monitorización de la actividad neuronal, se produce una ausencia de regulación sectorial específica que proporcione garantías adecuadas para dichos tratamientos, lo que viene a suscitar importantes preocupaciones éticas y jurídicas sobre el impacto final en principios, derechos y libertades fundamentales como la dignidad humana, el libre desarrollo de la personalidad, la identidad y la autonomía, el derecho a la intimidad, la libertad de pensamiento y de expresión, la integridad física y psíquica, la salud física y mental, etc. motivos por los que la Declaración crea un Grupo de Trabajo sectorial al objeto de analizar las bases jurídicas de los trata-

mientos en función de su finalidad, sus principios, límites y garantías aplicables en el marco de la normativa de protección de datos personales al tratamiento de neurodatos.

La AEPD también impulsó la protección de los neuroderechos en el seno de las actividades del **Grupo de Berlín**, participando en la elaboración de varios documentos en los que se exploraron los riesgos que pueden presentar estas tecnologías combinadas con otras como la realidad extendida, los Grandes Modelos de Lenguaje (LLM) en IA.

A estas acciones se suma también la participación de la AEPD en los **grupos ISO** donde se aporta la experiencia y el conocimiento en esta materia a modelos de normas que en el futuro puedan convertirse en estándares de los sectores de actividad en los que estas tecnologías tendrán aplicación.

En definitiva, la AEPD entabló un diálogo activo con expertos en neurociencia, tecnología, ética y derecho, así como con representantes del sector privado y público, para comprender en profundidad las implicaciones del tratamiento de neurodatos y proporcionar directrices y orientaciones para abordar el principio de responsabilidad activa del RGPD. Estas colaboraciones permitieron recoger diferentes perspectivas y enriquecer el debate sobre cómo interpretar y aplicar el RGPD en este contexto tan complejo.

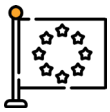
Es nuestra intención priorizar la regulación, estandarización y supervisión de este tipo de tratamientos de datos personales en colaboración con diferentes autoridades y organismos internacionales ya que se debe evitar que la neurotecnología se utilice, por ejemplo, para perfilar a la ciudadanía o para manipular sus comportamientos o decisiones.

CÓDIGOS DE CONDUCTA

El pasado 17 de diciembre de 2024 la AEPD aprobó el "**Código de conducta para la regulación de controversias de protección de datos en el sector de las comunicaciones electrónica**s", promovido por las operadoras de telefonía de los grupos Orange, Telefónica, Vodafone y MásMóvil. Este código, cuya adhesión es voluntaria pero vinculante para las entidades adheridas, constituye una muestra de autorregulación y un procedimiento de mediación ágil (plazo máximo de duración 30 días) y gratuito para la ciudadanía, con el objetivo de que las dos partes, ciudadanos/as y entidades adheridas al código, alcancen un acuerdo sin tener que recurrir a un procedimiento administrativo o judicial para resolver su conflicto. Durante el año 2025 la Agencia analizará el impacto que puede tener el Código de conducta en el desarrollo de las funciones que desarrolla la propia Agencia, así como en una eventual disminución de los ingresos económicos que vienen derivándose de la imposición de sanciones a las empresas que han promovido el Código.

ÁMBITO INTERNACIONAL

A nivel internacional, es particularmente destacable cómo la reciente adopción del paquete legislativo digital ha impactado considerablemente sobre el RGPD y la actividad del Comité Europeo de Protección de Datos (EDPB).



Efectivamente, la protección de datos permea la prestación de servicios digitales como una dimensión transversal de los nuevos Reglamentos europeos, *Digital Services Act* (DSA), *Digital Markets Act* (DMA), *Data Governance Act (*DGA) y *Artificial Intelligence Act* (AIA), cuya interrelación con el RGPD es evidente al atribuir a las autoridades de protección de datos nacionales nuevas funciones y competencias.

Durante 2024, en el seno del EDPB se trabajó en diferentes proyectos, como el desarrollo de unos ***Principios europeos de alto nivel para sistemas de verificación de edad***, basados en el decálogo que elaboró la AEPD en 2023; el desarrollo de las ***Directrices sobre blockchain***; la elaboración de las ***Directrices sobre acceso biométrico a servicios físicos*** como entornos laborales, gimnasios o

estadios; el ***Dictamen sobre el consentimiento válido en el contexto de los modelos de consentimiento o pago aplicados por servicios digitales que no son grandes plataformas en línea***, típicamente periódicos online. En relación con las plataformas de gran tamaño, alguna de ellas anunció un cambio en su modelo de negocio, ofreciendo una opción de "experiencia menos personalizada" que incorporaba un tratamiento menos intensivo de datos personales, lo que demostró el buen hacer del Comité.

BIOMETRÍA

En relación con el tratamiento de **datos biométricos**, ha de destacarse que como consecuencia de la medida cautelar de cese temporal de actividad durante 3 meses de una entidad con sede principal en Baviera, que realizaba tratamientos de datos biométricos en España, **la Agencia lideró la negociación** con la autoridad de protección de datos de dicho Estado, consiguiendo una resolución final tras el compromiso jurídicamente vinculante de paralización de actividad de la empresa en España hasta finales de 2024.

Asimismo, en 2024 destacaron algunos resultados en el seno del EDPB, como el ***Dictamen 11/2004 sobre el uso del reconocimiento facial para agilizar el flujo de pasajeros en los aeropuertos, el Dictamen 08/2024 sobre el consentimiento válido en el contexto de los modelos de consentimiento o pago aplicados por las grandes plataformas en línea, defendiendo la posibilidad de incluir*** una tercera vía gratuita sin rastreo (ej. publicidad contextual sobre temas elegidos por el usuario); o la ***Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco del Reglamento de Inteligencia Artificial***, no sólo como responsables del cumplimiento de la normativa en materia de protección de datos sino también como eventuales autoridades de vigilancia de mercado de sistemas de inteligencia artificial de alto riesgo, tales como sistemas de identificación biométrica en entornos fronterizos.

RED IBEROAMERICANA

En el ámbito de la Red Iberoamericana de Protección de Datos, durante 2024 se reforzaron las alianzas con organismos como la UNESCO, con quien se firmó una Carta de Intenciones para colaborar en el ámbito de la IA y de las neurotecnologías, y la SEGIB, con quien se firmó un Memorandum de Entendimiento para la actualización de los estándares iberoamericanos de protección de datos, adaptándolos a la realidad de las nuevas tecnologías y cuyo informe se presentó en la Cumbre de Jefas y Jefes de Estado y de Gobierno desarrollada a finales de 2024 en Ecuador.

Cabe destacar también la celebración del XXI Encuentro Iberoamericano de protección de datos celebrado en 2024 en Cartagena de Indias, Colombia, donde se debatió sobre los desafíos derivados del uso de las tecnologías emergentes con relación a la formulación de propuestas de políticas públicas específicas para promover el fortalecimiento de la protección de los datos personales y la privacidad, así como su uso ético y responsable.

Prueba de ello son los cuatro grupos de trabajo creados a tal fin: ChatGPT, Worldcoin, Neurodatos y Violencia Digital y Salud Digital, en el que se prestó una particular dedicación en torno a la protección de los colectivos más vulnerables, especialmente el de los y las menores de edad en el mundo online, formulando propuestas de herramientas no intrusivas que permitan mejorar la protección de su privacidad.

2. Desafíos para la privacidad

La Hoy en día somos testigos del crecimiento exponencial que ha experimentado la tecnología de **aprendizaje automático (machine learning)** y la **inteligencia artificial (IA)** en general y de la intención de la regulación europea de evitar consecuencias negativas sobre el estado de derecho. La regulación ha sido un imperativo de la evolución de estas tecnologías por parte de la Comisión Europea y, tanto en Europa como a nivel internacional, ha tenido un especial énfasis el papel desempeñado por la AEPD.

2.1 El Reglamento de Inteligencia Artificial (RIA)

Esta norma marca un hito importante en la regulación de la IA en el mercado único europeo, su implementación será gradual, permitiendo que las organizaciones se ajusten a los nuevos requisitos.

La regulación de la IA es un desafío complejo que requiere un enfoque multidisciplinar y una colaboración continua entre los diferentes actores involucrados. El RIA representa un avance significativo en este ámbito, pero su implementación efectiva dependerá de la capacidad de las organizaciones para adaptarse a las nuevas normativas y de la cooperación entre las autoridades reguladoras.

2.2 Datos genéticos

Un segundo desafío destacable son los avances tecnológicos en el análisis de **datos genéticos** y el amplio abanico de posibilidades que han abierto en diferentes áreas, desde aplicaciones comerciales hasta su uso para una asistencia clínica y en proyectos de investigación. Sin embargo, estas innovaciones también plantean una serie de desafíos en cuanto a la privacidad y protección de los datos personales, lo que requiere una reflexión profunda sobre los posibles impactos de su uso en diversos contextos. Los datos genéticos, por su naturaleza, son datos personales altamente sensibles, con características intrínsecas que deben ser analizadas cuidadosamente desde una perspectiva de protección de datos, dada su capacidad para revelar información muy detallada sobre la salud y las predisposiciones genéticas personales.

Para abordar estos desafíos, se considera imprescindible contar con la colaboración de profesionales especializados en el sector de la genética, la protección de datos y la ética, quienes podrán aportar diversas perspectivas sobre cómo gestionar de manera responsable los datos genéticos, garantizando que su uso sea respetuoso con los derechos de la ciudadanía y conforme a la legislación vigente. Esta interacción es clave para desarrollar soluciones que promuevan la innovación tecnológica como la protección de la privacidad de las personas.

En este contexto, la AEPD se ha unido a la iniciativa del Consejo de Transparencia y Protección de Datos de la Junta de Andalucía que ha impulsado el proyecto de “Espacio de Datos sobre Genética”, con el objetivo de establecer un espacio de trabajo que permita abordar de manera conjunta y efectiva los retos que plantea el uso de los datos genéticos. Este proyecto es análogo al Espacio de Datos sobre IA, ofreciendo un entorno de análisis y reflexión sobre las implicaciones legales, éticas y de privacidad en el manejo de los datos genéticos.

2.3 Interacción normativa

La interacción entre el Reglamento de IA y el RGPD afecta a aspectos críticos como el análisis de riesgos, las evaluaciones de impacto y el consentimiento informado. El Reglamento de IA exige una evaluación de impacto sobre derechos fundamentales para sistemas de alto riesgo, mientras que el RGPD establece la obligación de realizar evaluaciones de impacto en protección de datos personales. Ambos marcos normativos imponen requisitos de consentimiento explícito: en el Reglamento de IA para pruebas reales con datos personales y en el RGPD para su tratamiento en dichos sistemas.

La jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) y las directrices del Supervisor Europeo de Protección de Datos (SEPD) confirman que toda normativa que implique tratamiento de datos personales debe acompañarse de una evaluación de impacto para determinar sus riesgos y garantizar su proporcionalidad, idoneidad y necesidad. La mera existencia de operaciones de tratamiento previstas por la

legislación supone una restricción del derecho a la protección de datos, aunque dicha restricción pueda justificarse.

En este contexto, la Agencia ha elaborado directrices detalladas para identificar los casos en que se debe llevar a cabo una evaluación de impacto. Estas incluyen el análisis del rango normativo, la identificación de riesgos para los derechos fundamentales, la proporcionalidad de las medidas propuestas y la implementación de mecanismos para mitigar dichos riesgos.

Asimismo, la AEPD propone que todas las disposiciones normativas de carácter general incorporen una cláusula específica sobre protección de datos, facilitando la correcta interpretación y aplicación de las obligaciones derivadas del RGPD en el desarrollo normativo.

2.4 Ámbito internacional

Por otro lado, en el **ámbito internacional**, la Agencia seguirá desarrollando dos líneas de trabajo concretas: por un lado, a nivel europeo, en torno al EDPB y sus subgrupos de trabajo, en los que la Agencia, además de definir criterios interpretativos de la normativa de protección de datos y colaborar en la elaboración de directrices y opiniones del EDPB, lidera algunas materias como Blockchain, Acceso Biométrico y Verificación de Edad.

Y, por otro lado, en el ámbito de la Red Iberoamericana de Protección de Datos (RIPD), cabe destacar la constitución de cuatro grupos de trabajo, a iniciativa de la AEPD, que requieren del impulso y colaboración activa entre las autoridades de protección de datos: Neurodatos, Violencia Digital, WorldCoin y ChatGPT. Además, sería conveniente en el futuro, establecer colaboraciones con otras redes regionales como por ejemplo la africana.

A estas dos líneas de trabajo habría que añadir dos líneas en relación con el Consejo de Europa, para afrontar la adopción del denominado Convenio 108+, que posiblemente entre en vigor a lo largo de 2025, y el desarrollo del Convenio sobre Inteligencia Artificial. Y, por otro lado, respecto a la OCDE, la AEPD se ha incorporado recientemente a dos grupos de trabajo, uno sobre gobernanza de protección de datos y otro sobre inteligencia artificial.

A los proyectos anteriores cabe añadir una línea adicional de nueva creación, que surgiría en caso de que la AEPD fuera designada Autoridad de Vigilancia de Mercado del Reglamento de Inteligencia Artificial (AIA), lo que requeriría de un análisis pormenorizado y de flexibilidad, dado que al tratarse de una materia nueva necesitará de un proceso de maduración.

En definitiva, las cuestiones que se encuentran en desarrollo y que requerirán de un impulso mayor a lo largo del 2025, son las relacionadas con la IA, tanto en lo que afecta a la Decisión de la posible designación de la AEPD como Autoridad de Vigilancia de Mercado, como hacer un seguimiento de la implementación del tratamiento de incidentes graves de sistemas de IA, integrarse en los grupos de la Competent Authorities in Artificial Intelligence específicamente de notificación de incidentes y transparencias, participar en el EDPB interplay GDPR-AIA, colaborar en el desarrollo de los mecanismos de identidad digital con relación al eIDAS2 y la cartera digital europea, así como el desarrollo de orientaciones y la participación en organismos internacionales en lo relativo a neurodatos, datos genéticos o biométricos.

Asimismo, es de enorme importancia la automatización de la gestión de brechas de datos personales para hacer frente al incremento de las notificaciones de forma eficiente, para servir de protección a los interesados y de apoyo a los responsables; el impulso y actualización de las guías, orientaciones y herramientas de gestión del riesgo y evaluación de impacto, con un enfoque más práctico y desplegando un análisis formal de las amenazas en protección de datos, en línea con los estándares y la industria, así como actualizar las herramientas Notifica y Comunica Brecha para proporcionar una nueva herramienta inter-autonómica.

En líneas de trabajo paralelas, resulta relevante la actualización de las guías y recursos de ayuda con relación a los tratamientos de datos y la participación internacional en el desarrollo normativo nacional y europeo alrededor de los datos, como la DGA, DMA, DSA, DA, los futuros Reglamentos de Espacios de Datos, en particular el Espacio Europeo de Datos de Salud; la colaboración con Alastria para la implementación de Blockchain-RGPD y la actualización de las herramientas orientadas específicamente a PYMES, como

Facilita y Facilita-Emprende para abarcar las necesidades de grupos más amplios de entidades y actividades de formación en colaboración con asociaciones profesionales.

Del mismo modo pretende abordar aspectos relevantes en los escenarios de acceso a cantidades masivas de datos, y en particular sobre datos sanitarios, comenzando en un futuro próximo con la propuesta ya presentada junto con la autoridad de protección de datos griega en el marco de trabajo de ENISA DPE AHWG sobre consideraciones de protección de datos en los entornos de procesamiento seguro que recoge la propuesta de Reglamento del Espacio Europeo de Datos Sanitario.

En este punto no se puede dejar de señalar la necesaria colaboración con el Ministerio de Transformación Digital y en concreto con la Dirección General del Dato (antigua Oficina del Dato) y la Agencia Española de Supervisión de Inteligencia Artificial (AESIA).

2.5 Retos de futuro

Desde el punto de vista de la **planificación**, pero no menos importante que los desafíos mencionados anteriormente y que será uno de los primeros retos que abordará la primera Presidencia de la Agencia, después de seis direcciones que le han precedido, será la aprobación del **Plan Estratégico 2025-2030**, que determinará las líneas de actuación de la AEPD en dicho período, incorporando las acciones específicas propuestas por cada departamento del organismo en relación con sus respectivas materias, así como una planificación estratégica acorde de recursos humanos y de programación de la contratación y presupuestación.

Asimismo, la labor de la Agencia de supervisar la aplicación de la normativa de protección de datos personales ha de verse plasmada, entre otras acciones, con la adopción de **planes de acción bienales** dirigidos al cumplimiento de sus obligaciones por parte de los responsables y encargados de tratamientos, previas reuniones con los sectores estratégicos en materia de protección de datos (sanidad, educación, telecomunicaciones, seguros, banca, gran consumo, suministros básicos -luz, agua, gas-, Administraciones Públicas, etc.). La actividad de la Agencia ciertamente versa sobre muchas actuaciones en estos sectores, si bien, obviamente, sin abordar la protección de derechos del ámbito de consumo, por ejemplo, que no sean claramente conectados con la protección de datos.

En este sentido, uno de los ejes principales de las actuaciones de la AEPD es el que se enmarca dentro de lo previsto en el RGPD y 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 promoviendo la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos. Sin duda, la Agencia va a dar un salto adelante en este ámbito favoreciendo una mayor y más intensa colaboración.

En línea con lo anterior y dentro de su tarea de **apoyo y sensibilización** a las Pymes y micropymes para el cumplimiento de las obligaciones en materia de protección de datos, la AEPD insistirá, de acuerdo con lo establecido en el RGPD, en la importancia de designar por parte de los responsables y encargados de los tratamientos a delegados de protección de datos, reforzando y apoyando esta figura a través de encuentros periódicos y analizando su situación de forma periódica.

Finalmente, cabe mencionar que la Agencia continuará desarrollando una serie de **estrategias** para hacer frente al gran aumento de trabajo, basadas en tres ejes fundamentales: la adecuación de la plantilla (teniendo en cuenta que el incremento exponencial de las reclamaciones gestionadas por la Agencia no es acorde con el incremento de su personal); la simplificación y automatización de procedimientos (lo que conlleva un aumento de productividad y una reducción de los tiempos de tramitación) y las modificaciones normativas, no sólo las que afectan al Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, sino también a la LOPDGDD, sobre aspectos relacionados con el deber de colaboración y las competencias propias de la Agencia, así como

la legitimación del tratamiento de datos por los sistemas de exclusión publicitaria y sin duda, el uso de la Inteligencia Artificial, dando ejemplo de ello.

En este sentido habrá que tener en cuenta el impacto que pueda tener el Reglamento de Inteligencia Artificial en relación con la actividad de la Agencia y las nuevas competencias que ésta pudiera adquirir, tanto a nivel nacional como internacional, en cuyo caso debería plantearse un importante incremento de la plantilla actual para asumir tales retos.

2.6 Jurídicos

2.6.1. Consultas

En el año 2024 se observa una tendencia continuista respecto del ejercicio anterior en la actividad del Gabinete Jurídico, que se ha centrado principalmente en la emisión de informes preceptivos sobre disposiciones legales y reglamentarias.

En segundo término, hay que citar la resolución de consultas en aquellos otros asuntos de carácter general en materia de protección de datos que, o bien no debían ser atendidas por el Canal DPD de la Agencia, o bien, porque eran de tal relevancia que hacían necesario el pronunciamiento del Gabinete, como expresión del criterio de la Agencia, para dotar de garantías y seguridad jurídica no sólo a los obligados por la norma sino también a los ciudadanos titulares de este derecho fundamental.

Todo ello de acuerdo con 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.

Entrando ya en las materias en las que el Gabinete Jurídico ha intervenido en su labor consultiva, hay que citar en primer lugar, **los informes sobre las categorías especiales de datos**.

El **Informe 17/2024** aborda la cesión de datos personales de salud de varias bases de datos, a la Autoridad Independiente de Responsabilidad Fiscal (en adelante AIREF) de cuyo tratamiento es responsable el Ministerio de Sanidad, a los efectos de llevar a cabo un "estudio de evaluación sobre la asistencia sanitaria del mutualismo administrativo, acerca de los efectos sobre la salud de los mutualistas y el gasto público en términos de eficiencia".

Con base a un Acuerdo del Consejo de Ministros, la AIREF plantea la autorización para que las bases de datos sean cruzadas un entorno de tratamiento seguro por la Agencia Estatal de Administración Tributaria (AEAT), con bases de datos de otros Departamentos, de la propia AEAT y entidades dependientes de la AGE, como las mutualidades de funcionarios.

En el informe se recuerda la doctrina del Tribunal Constitucional (por todas la STC 76/2019 de 22 de mayo) y del Tribunal de Justicia de la UE, sobre el tratamiento de las categorías especiales de datos y sobre las cesiones de datos en general (STJUE C.201/14 de 1 de octubre de 2015) y el Considerando 31 del RGPD, referido a que, *Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento*. El informe concluye que la solicitud de cesión de datos objeto de esta consulta no trae causa de una norma legal con el alcance y contenido que establece la jurisprudencia afectada sino de un Acuerdo del Consejo de Ministros, cuyas previsiones carecen del valor normativo necesario para habilitar los tratamientos de datos solicitados. Del mismo modo, tampoco es posible considerar como título habilitante suficiente para permitir la realización de esta consulta las previsiones contenidas en la LO 6/2013, de 14 de noviembre, de creación de la Autoridad Independiente de Responsabilidad Fiscal. Por todo ello el criterio de la AEPD no es favorable a la cesión planteada.

Siguiendo con las categorías especiales de datos, el **Informe 29/2024** analiza la posibilidad de que las entidades gestoras y servicios comunes de la Seguridad Social puedan comunicar al Instituto Nacional de Estadística (INE) categorías especiales de datos (en particular, datos de salud) para que dicho Instituto lleve a cabo una operación estadística incluida en el Plan Estadístico Nacional.

Los datos que estarían comprometidos por la cesión estarían bajo la protección del artículo 9 del RGPD por cuanto se solicita el tipo de prestación percibida por los ciudadanos de la que se pueden deducir categorías especiales de datos.

El informe, tras recordar el criterio de la Agencia sobre el tratamiento de este tipo de datos en las consultas, encuestas y estadísticas, concluye que corresponde al INE demostrar que dicha información solicitada es requerida (juicio de necesidad) por la norma legal habilitante (nacional o europea), y que es adecuada, pertinente y no excesiva (juicio de proporcionalidad) respecto de la finalidad concreta establecida para dicha estadística.

Estableciendo que corresponderá al INE fundamentar en este caso en concreto en qué manera la variable tipo de prestación que solicita es necesaria o proporcional en sentido estricto a los efectos de los fines de dicha estadística, hasta el punto de justificar la solicitud de dichos datos de salud, sin olvidar la previsión de aportación estrictamente voluntaria y previo consentimiento expreso de los interesados prevista en el artículo 11.2 LFPE.

En definitiva, se hace una interpretación estricta respecto de los datos personales sensibles que se permite recoger de fuentes distintas a los interesados, dado que si cuando se recaban los datos directamente de los interesados se requiere su consentimiento expreso, la solicitud de tales datos a terceros ha de ceñirse estrictamente a los establecido en la norma legal (europea o nacional) cuando ésta establezca la necesidad de dichos datos, y en la manera en que lo establezca, siempre que sea apropiado, pertinente y no excesivo a los fines pretendidos por la estadística concreta que se pretende cumplimentar.

Fuera de estos casos, esto es, existiendo algún tipo de duda razonable acerca del requerido juicio de necesidad y de proporcionalidad, con base en la interpretación estricta que afecta a la cesión de datos personales especialmente protegidos, procedería realizar la comunicación de tales datos de manera anonimizada.

Destaca el **Informe 46/2024** que trata de dar solución a una consulta recibida en el Ministerio de Sanidad sobre una petición realizada al amparo de la ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (en adelante, ley 19/2013), y de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, que recae específicamente sobre información atinente a datos de salud.

En concreto se refiere a:

- *El registro anonimizado de ingresos en los hospitales públicos españoles (con provincia del hospital) por TODOS y cada uno de los motivos que corresponden a todas las categorías de salud que existen (y que están contempladas en los manuales de salud con los códigos CIE).*

- *Los datos han de estar desglosados para los años 2011 hasta diciembre de 2023 para todos y cada uno de los años.*

- *Indicación expresa del sexo y de la edad concreta persona ingresada, la edad concreta fecha de ingreso exacto (día, mes, año) y fecha de alta (día, mes, año).*

- *Si de cada ingreso fue por urgencias o fue un ingreso programado y la resolución final del caso: alta a domicilio, traslado a otro hospital, alta voluntaria....*

El informe considera que la información se centra en determinados datos que con el nivel de agregación solicitado conllevaría un riesgo de identificación de las personas afectadas. Aunque se indica que se piden datos anonimizados, en realidad se trata de datos desidentificados, que podrían ser

reidentificados sin mucho esfuerzo, cruzando la información solicitada con otros datos fácilmente obtenibles de registros o fuentes públicas, dado el nivel de detalle de los datos que se solicitan.

(…) *Nos encontramos, por tanto, en opinión de esta Agencia, ante una solicitud de datos desidentificados, que no anonimizados* (…) señala expresamente el informe. Y por tanto los datos solicitados por la petición de transparencia se encuentran incluidos en el concepto de "datos personales" del art. 4.1 RGPD.

En relación con la Ley 19/2013, dice el informe que (…) *se contiene una regulación específica cuando la documentación a la que hace referencia el derecho de acceso a la información pública contiene datos personales de salud, y que el responsable del tratamiento habrá de cumplir. Dicha regulación ha sido añadida, expresamente, por la disposición final 11.2 de la LOPDGDD. En concreto el art. 15.1, párrafo segundo, de la ley 19/2013, impide al responsable del tratamiento, en este caso la Administración pública a la que se ha solicitado el acceso a datos personales de salud, llevar a cabo el tratamiento consistente en la cesión de datos al solicitante si no se cuenta con el consentimiento del afectado o si el solicitante estuviera amparado por una norma con rango de ley. No se considera aplicable tampoco la excepción a la excepción prevista en el apartado 4 del art. 15, por cuanto, de acuerdo con la opinión del responsable del tratamiento, la agregación de la información en la forma solicitada no haría posible tal disociación que impida la identificación de las personas afectadas, sino que ello conlleva un riesgo efectivo de reidentificación. Por tanto, ninguna de estas circunstancias que excepcionan la prohibición se dan, luego el Ministerio requerido no podría ceder (tratar) la información solicitada para su cesión al requirente por cuanto contendría datos especialmente protegidos, de salud.* (…).

También se indica en el informe que la fuente de datos de la información solicitada, esto es, Registro de Atención Especializada (RAE-CMBD), y su explotación, forma parte del conjunto de operaciones estadísticas del Plan Estadístico Nacional y por tanto le es de aplicación la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y que de acuerdo con los artículos 13.2 y 3, 14.2 y 15.3, la información solicitada por la vía de la ley de Transparencia está, igualmente, sujeta al secreto estadístico, y no es posible divulgarla salvo si se dieran los requisitos previstos en esta norma, que no consta que existan.

Por todo ello, el informe adopta las **siguientes conclusiones**:

1) Es apropiado valorar el riesgo de reidentificación como criterio fundamental para denegar, acceder a la petición o modular qué datos y cómo se ceden en solicitudes que conlleven reelaboración de los datos personales de salud de que dispone el Ministerio al amparo de la Ley de Transparencia y Buen Gobierno, cuando al amparo de dicha reelaboración dicha información que se cede al solicitante pueda contener datos personales de salud. En esos casos, habrán de seguirse los criterios establecidos en el art. 15 de la ley de Transparencia para poder ceder la información.

2) Es apropiado que el Ministerio de Sanidad deniegue aquellas solicitudes efectuadas al amparo de la Ley de Transparencia y Buen Gobierno en las que se solicitan datos personales especialmente protegidos incluidos en el art. 15.1, segundo párrafo, de dicha ley de Transparencia, cuando no se den las causas que permiten levantar dicha prohibición.

3) Cuando exista una normativa sectorial específica que conlleve una regulación propia del acceso a la información, la Ley de Transparencia sólo es de aplicación supletoria, y deberá de tenerse primeramente en cuenta, para el acceso a la información solicitada, la aplicación de la normativa especial.

4) Corresponde al Ministerio de Sanidad, en tanto que responsable del tratamiento de datos personales en que consistiría la anonimización de datos personales en su poder, que dicho tratamiento cumpla efectivamente con los requisitos necesarios para dicha anonimización, evitando que un tratamiento posterior de dichos datos una vez anonimizados pueda dar lugar a su reversión de manera que un tercero pueda tener acceso a los datos personales.

El **Informe 21/2024** analiza el tratamiento de datos para llevar a cabo una Macroencuesta de Violencia contra la Mujer, encuesta oficial y que se encuentra incluida el Plan Estadístico Nacional 2021-2024, con código 8921. Se pretende obtener de la CNMC los números de teléfonos de las mujeres incluidas en la muestra teórica, "incluso aunque estas hayan hecho uso de su derecho de oposición a figurar en los listados de teléfonos".

En la solicitud se indica que la recogida de los datos necesarios para dicha encuesta se llevará a cabo a través de lo que denomina método multicanal, y más específicamente a través de recogida mediante internet (denominada CAWI) y presencial (denominada CAPI). La utilización del teléfono (denominada CATI) "sólo está prevista [como medio] de incentivación telefónica para animar a las mujeres a que respondan por internet".

El informe parte del análisis de que estamos ante el tratamiento de datos para fines estadísticos y la necesidad de que la existencia de al menos una base de legitimación del artículo 6 del RGPD y la observancia de los principios del tratamiento, en especial el de minimización. Asimismo, recuerda que finalidad estadística es, asimismo, una de las circunstancias que permiten levantar la prohibición de tratamiento de categorías especiales de datos establecida en el art. 9.1 RGPD. Más en concreto, el art. 9.2.j) *RGPD especifica que ello será así cuando sea "necesario" sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. En el caso de la Macroencuesta de Violencia contra la Mujer, los datos (principales variables) que se recogerían serían: "Violencia declarada alguna vez en su vida, violencia declara en el último año, frecuencia, severidad, tipo de agresor (entre otras)". Tanto la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en su art. 25.2, segundo inciso, como Ley 12/1989, de 9 de mayo, de la Función Estadística Pública en su art. 11, señalan que serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679, especificando aún más la ley 12/1989 para todas aquellas circunstancias que puedan afectar a la intimidad personal o familiar. Cabe considerar que los datos a los que se refiere la encuesta (datos sobre violencia de género) entran dentro de esta categoría, por lo que su aportación será exclusivamente voluntaria*.

Tras analizar la normativa de la CNMC para la cesión de datos, la voluntariedad de cumplimiento de la encuesta, así como la finalidad del tratamiento en cuestión, el informe concluye que *el tratamiento del dato personal del número de teléfono de las personas, que esta Agencia considera extremadamente intrusivo, sin contar con la aquiescencia de la persona afectada, sería, en opinión de esta Agencia, un tratamiento que no cumpliría el principio de minimización de datos del art. 5.1.c) RGPD, por cuanto no se considera esencial para la realización de la encuesta, ya que esta se lleva a cabo por otros canales (CAWI, CAPI), y su utilización se pretende por el consultante para "incentivar" y "animar" a proporcionar unos datos que son estrictamente voluntarios, y que por lo tanto no necesitarían de dicha "incentivación", o cuando menos no se considera estrictamente "necesaria" la misma desde la perspectiva de la protección de datos personales, circunstancia esta que se requiere, conforme al ya citado art. 9.2.j) RGPD, para considerar levantada la prohibición de tratamiento de datos sensibles para dichas finalidades*. En consecuencia, el sentido del informe es desfavorable al tratamiento propuesto.

También relacionado con la Ley de Transparencia y la protección de datos personales, se emitió el **Informe 58/2024** que aborda la consulta realizada por el Ayuntamiento de Olite, en relación con la petición que realiza un miembro de la corporación municipal solicitando en calidad de concejala la información sobre el Registro del Ayuntamiento, en concreto el extracto de las entradas y salidas durante "el mes de mayo", con indicación del número de registro, fecha, quién lo presenta, a quién va dirigido, breve descripción del asunto. En la petición no se indica la finalidad concreta.

El informe comienza haciendo una reflexión sobre la consideración de dato personal de la información solicitada, que va más allá de la identificación de la persona que presenta un documento en el registro de la corporación local, e incluso puede contener categorías especiales de datos.

Posteriormente se analiza también la aplicación de las leyes de transparencia, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y a nivel autonómico de Navarra en la Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno, para concluir que, (…) ,correspondería al Ayuntamiento consultante determinar en primer lugar si *la información solicitada incluye datos de carácter personal; en su caso determinar si es especialmente protegida, bien según el art. 15.1, primer apartado, en cuyo caso será necesario en todo caso consentimiento expreso y por escrito de cada interesado; si es del art. 15.1, segundo apartado, se necesita consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley. Si no contuviera datos especialmente protegidos, aun así deberá realizar una ponderación teniendo en cuenta particularmente la justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos (no se alega nada al respecto); el menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos (en opinión de esta Agencia, los documentos solicitados pueden contener datos personales que afecten de manera intensa al derecho fundamental a la protección de datos, dado que una solicitud a la Administración necesariamente ha de contener, cuanto menos, la identificación pero además los hechos, razones y petición en que se concrete la solicitud (art. 66 ley 39/2015), lo que supone que un tercero pueda conocer las razones y las peticiones que se solicitan a la Administración, que pueden ser amplísimos, y, más aún, el tercero podrá conocer los actos administrativos de concesión de derechos/autorizaciones etc. de la Administración a un tercero. El Ayuntamiento también deberá tener en cuenta "la mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad". Y, además, y en todo caso, el art. 19.3 de la ley 19/2013 establece la necesidad de que, si la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El traslado de la solicitud al afectado producirá la suspensión del plazo para resolver hasta que se reciban las alegaciones o transcurra el plazo para su presentación. El solicitante deberá ser informado de esta circunstancia. Si el tercero no responde en el plazo requerido se presumirá su disconformidad con que se otorgue el acceso a la información solicitada*.

Se trata de cuestiones que sin duda habría que revisar y analizar de manera más armonizada con los criterios de las diversas autoridades competentes e independientes y teniendo en cuenta los derechos fundamentales de los concejales afectados, que forman parte además de la propia administración municipal.

En cuanto a los principios del tratamiento, en el Informe 37/2024 se analiza la adecuación a los principios de finalidad y minimización de datos el tratamiento de datos personales que se realiza tanto en los procesos selectivos como en los procesos de provisión de puestos de trabajo en las administraciones públicas.

El informe confirma el criterio adoptado en el Informe 2/2022 sobré cómo conjugar los principios de protección de datos con los de publicidad, transparencia, mérito y capacidad que han de informar el acceso a la función pública.

Comienza por aclarar el objeto del mismo en relación con la Sentencia de 26 de abril de 2012 de la Sección Primera de la Sala de lo Contencioso Administrativo de la Audiencia Nacional que se ha citado en numerosas ocasiones cuando se plantean las bases jurídicas que legitiman el tratamiento de datos en los procesos selectivos indicando que para excluirla del análisis que se realiza en el informe, al indicar que (…)*lo indicado en la Sentencia no opera en la consulta hoy planteada por cuanto no se está analizando la concurrencia del principio de licitud para, con carácter general, someter a tratamiento los datos personales de los participantes en un proceso*

selectivo, cuestión que ya se solventó en nuestro Informe 86/2020(…) lo que aquí se plantea es el análisis no sólo del principio de licitud, sino también de otros de igual relevancia como el principio de limitación de la finalidad o el de minimización, ambos expresión del principio proporcionalidad, sin olvidarnos de la aplicación de medidas de protección de datos desde el diseño y por defecto. (…).

El debate que se plantea es sobre quién puede acceder a las publicaciones de los actos del proceso selectivo que contengan datos personales de los aspirantes, si el público en general o únicamente éstos.

Basándose en el concepto de interesado, y en la legitimación procesal para impugnar los actos del proceso, se afirma que (…) *la publicación "en abierto" de los listados de admitidos y excluidos, así como de otros trámites internos del proceso selectivo, como calificaciones, resultado de baremación de méritos, lugar, día y hora para lectura de ejercicios, etc., de acuerdo con el principio de finalidad y pleno respeto al principio de minimización, únicamente conciernen a los interesados en el procedimiento, que son los participantes en el mismo.(...) el conocimiento de los trámites por los que pasa el proceso selectivo, incluyendo la información susceptible de ser considerada dato personal, tiene como finalidad -como se ha indicado, con carácter general, y salvo aquellos supuestos que los principios de publicidad y transparencia puedan justificar- facilitar el ejercicio de medios de impugnación y revisión, cómputos de plazos, etc., es decir, cuestiones que escapan a la necesidad del conocimiento de terceros por cuanto no tienen legitimación para conocer dicha información al no ser interesados. Esa falta de legitimación es coherente con la falta de legitimación en el proceso contencioso administrativo que se sustanciaría tras una eventual impugnación en vía administrativa de los actos internos del proceso selectivo.* (…).

El informe reitera el criterio seguido en anteriores ocasiones cuyo contenido, en síntesis, el siguiente:

- *La publicación de los actos internos del proceso selectivo, de manera completa y que por tanto contenga datos de carácter personal y sin perjuicio de lo dispuesto en la disposición adicional séptima de la LOPDGDD, debe circunscribirse únicamente a los participantes en el mismo, que ostentan un evidente interés legítimo en conocer toda la información referida al mismo.*

- *Terceros ajenos al procedimiento, podrán acceder a las convocatorias del procedimiento selectivo, a las distintas resoluciones de las fases internas del proceso selectivo siempre y cuando no contenga información susceptible de ser calificada como dato personal -en este caso, o bien se prescinde absolutamente de listados, o bien, una medida adecuada seria el uso de un código alfanumérico asignado a los participantes al inscribirse en el proceso selectivo, o incluso a través del nº de instancia, que operaria como identificador personal en el proceso selectivo, y que manteniendo la consideración de dato personal en tanto seudonimizado (Considerando 26 RGPD), permitiría la coexistencia de dicho tratamiento con los principios de minimización y limitación de la finalidad-, y finalmente, a la resolución completa de los nombramientos como empleados públicos -en la que ya si figuran datos personales- y que revisten un evidente interés general.*

Y concluye respecto de las medidas concretas adoptar para conjugar los principios afectados, que en cualquier caso (…) *forma parte del principio de responsabilidad proactiva, del que es acreedor el responsable del tratamiento, adoptar aquellas que, de acuerdo con las especiales características de su organización y del tratamiento que vaya a realizar, estime como más acertadas sobre los criterios generales que se acaban de recordar*.

En el ámbito de los Códigos de Conducta, en este ejercicio se observa un descenso de informes en la materia, únicamente destaca el Informe 22/2024 sobre el "Código de Conducta para la Regulación de Controversias de Protección de Datos en el Sector de las Comunicaciones electrónicas"

2.6.2 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 cabe mencionar las siguientes:

1. Anteproyecto de Ley por la que se crea la Autoridad Administrativa Independiente de Defensa del Cliente Financiero para la resolución extrajudicial de conflictos entre las entidades financieras y sus clientes.

2. Anteproyecto de Ley por el que se modifica el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por Real Decreto Legislativo 8/2004, de 29 de octubre.

3. Anteproyecto de Ley de Industria y Autonomía Estratégica.

4. Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en entornos digitales.

5. Anteproyecto de Ley de prevención del consumo de alcohol y de sus efectos en las personas menores de edad.

6. Anteproyecto de Ley Administradores y Compradores de crédito.

7. Proyecto de Real Decreto Ley Establecimiento marco regulador general para tramitación procedimientos de concesión de ayudas con carácter de emergencia por los distintos Departamentos ministeriales, ante los daños causados por la DANA entre el 28 de octubre y el 4 de noviembre de 2024.

8. Segundo informe sobre el Anteproyecto de Ley de Administradores y Compradores de Crédito.

9. Proyecto de Real Decreto por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia, según lo dispuesto en el art. 94 de la Ley 13/2022, de 7 de julio, general de comunicación audiovisual.

10. Proyecto de Real Decreto por el que se regula la tramitación del DNI, el tratamiento de los datos de identidad y sus aspectos digitales.

11. Proyecto de Real Decreto por el que se aprueba el Estatuto de las personas cooperantes.

12. Proyecto de Real Decreto por el que se regula el pasaporte de servicio.

13. Proyecto de Real Decreto por el que se regula la publicidad de los productos sanitarios.

14. Proyecto de Real Decreto por el que se modifica el Real Decreto 962/2013, de 5 de diciembre, por el que se crea y regula el Consejo Estatal de la pequeña y la mediana empresa, y se crea y regula el Observatorio Estatal de la Morosidad Privada.

15. Proyecto de Real Decreto por el que se desarrolla la Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas en lo referido a la factura electrónica entre empresas y profesionales.

16. Proyecto de Real Decreto por el que se crea el Consejo de la Productividad de España.

17. Proyecto de Real Decreto por el que se aprueba el Estatuto de la Agencia Estatal de Administración Digital y se regulan la organización y los instrumentos operativos para la administración digital del sector público estatal.

18. Proyecto Real Decreto de modificación del Real Decreto 1614/2011, de 14 de noviembre de desarrollo de la Ley 13/2011, de 27 de mayo de Regulación del Juego, relativo a licencias, autorizaciones y registros del juego, para introducción de sistemas de límites de depósitos conjuntos por jugador.

19. Proyecto de Real Decreto por el que se aprueba el Estatuto de la Agencia Estatal Agencia Española de Cooperación Internacional para el Desarrollo.

20. Proyecto de Real Decreto por el que se aprueba el Reglamento de la Abogacía General del Estado.

21. Proyecto de Real Decreto por el que se regula la evaluación de tecnologías sanitarias.

22. Proyecto de Real Decreto por el que se regula el etiquetado accesible de productos de consumo.

23. Proyecto de Real Decreto por el que se regula el sistema de información de vacunaciones e inmunizaciones. SIVAIN.

24. Proyecto de Real Decreto por el que se modifica el Real Decreto 792/2023, de 24 de octubre, 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.

25. Proyecto de Real Decreto por el que se modifica el Reglamento del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor, aprobado por Real Decreto 1507/2008, de 12 de septiembre.

26. Proyecto de Real Decreto por el que se regula el uso y bienestar de los perros de asistencia.

27. Segundo informe sobre el Proyecto de Real Decreto por el que se modifica el Reglamento del seguro obligatorio de responsabilidad civil en la circulación de vehículos a motor, aprobado por el Real Decreto 1507/2008, de 12 de septiembre, después de correcciones.

28. Proyecto de Real Decreto por el que se aprueba el reglamento sobre las condiciones básicas de accesibilidad cognitiva.

29. Proyecto de Real Decreto por el que se modifica el Real Decreto 95/2009 de 06 de febrero, por el que se regula el Sistema de Registros Administrativos de Apoyo a la Administración de Justicia.

30. Informe sobre la constitucionalidad Ley 16/2023, de 21 de diciembre de la Autoridad Vasca de Protección de Datos.

31. Proyecto de Orden Ministerial de aprobación de la Política de Seguridad de la Información del Ministerio de Cultura.

32. Proyecto de Orden Ministerial por el que se crea la Plataforma Digital de Colaboración entre las Administraciones Públicas y se regula su configuración y funcionamiento.

33. Proyecto de Orden Ministerial por la que se regulan los cursos de sensibilización y reeducación vial para titulares de un permiso o licencia de conducción.

34. Proyecto de Orden Ministerial por la que se regula el Registro Electrónico de Apoderamientos de la Inspección de Trabajo y Seguridad Social.

35. Proyecto de Decreto por el que se aprueba la Política de Protección de Datos de la Administración de la Comunidad de la Illes Baleares.

36. Proyecto de Orden Ministerial por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migración y se crea el Comité de Seguridad de los Sistemas de Información.

37. Proyecto de Orden Ministerial por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración Digital del Ministerio de Hacienda.

38. Proyecto de Orden Ministerial por la que se modifica la regulación de la Comisión Ministerial de Administración Digital (CMAD) del Ministerio de Hacienda.

39. Proyecto de Orden Ministerial por la que se regula el uso de la firma electrónica para la certificación de las actuaciones de Traductores-Intérpretes Jurados, Traductores Jurados e Intérpretes Jurados.

40. Proyecto de Orden Ministerial por la que se regula la formación para el acceso progresivo al permiso de conducción de la clase A.

2.6.3 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 el 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 2024 se dictaron por la Sala de lo contencioso-administrativo de la **Audiencia Nacional**, 43 resoluciones, de las cuales:

- 21 fueron desestimatorias de los recursos formulados contra resoluciones de la Agencia (que quedaron plenamente confirmadas);
- 8 estimaron parcialmente el recurso;
- 3 estimaron íntegramente las pretensiones anulatorias de las resoluciones de la Agencia;
- y 11 inadmitieron los recursos interpuestos contra resoluciones de la Agencia.

Por su parte, el **Tribunal Supremo** dictó 9 resoluciones, de las cuales ocho de ellas confirmaron el criterio de la AEPD y la otra estimó las pretensiones de los recurrentes.

En cuanto a los sectores de actividad de los recursos, tanto en la Audiencia Nacional como en el Tribunal Supremo, de las resoluciones citadas, la mayor parte han sido interpuestos por particulares (28 de ellas en total)

No obstante, un alto número de ellas conllevan la declaración de inadmisibilidad, sin entrar si quiera en el fondo del asunto, ya que se aprecia la 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 y que el tribunal no es un órgano sancionador que pueda suplir la intervención de la Autoridad de Control y Supervisión, en este caso, la propia Agencia Española de Protección de Datos.

Les siguen las sentencias con fallo desestimatorio, 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 el tribunal, así como aquellas en las que la sala entiende la resolución suficientemente motivada. A los particulares les siguen aquellas resoluciones referidas al sector de las telecomunicaciones, después el sector banca y seguros y en igual medida los sectores energéticos, asociaciones y sindicatos, solvencia patrimonial y finalmente y en menor medida el sector de la distribución y venta.

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

Comenzando por aquellas resoluciones que tratan de los principios relativos al tratamiento de datos, procede citar la **Sentencia de 3 de octubre de 2024 recaída en el Recurso Núm. 990/2022** que aborda el **principio de licitud**, y también analiza la contratación a través de representación, en este caso, mediante poder notarial en una entidad financiera.

Concreta los hechos en que la persona afectada otorgó un poder general a favor de un tercero que le facultaba para representarla en distintos actos, entre otros actos, abrir cuentas corrientes o de crédito. Pero en ese documento notarial se advertía que la representación se otorgaba exclusivamente respecto de los bienes relacionados e integrados en la Comunidad de Bienes. El tercero incluyó a la afectada como cotitular en una cuenta corriente en la que figuraban otras dos personas físicas, y sin que dicha cuenta le correspondiera a la citada Comunidad de Bienes. El Banco de España frente al que se interpuso también la

correspondiente reclamación al amparo de la Ley 44/2002, de 22 de noviembre, y de la Orden ECC/2502/2012, confirmó la actuación negligente de la entidad financiera.

Recoge la Sentencia que: Para que la circunstancia del artículo 6.1.b) del RGPD pueda operar como base jurídica de un tratamiento de datos es presupuesto indispensable que quien intervenga como contratante o quien manifieste la intención de concluir un contrato y se identifique con determinados datos personales sea efectivamente el titular de los datos tratados. De no ser así, esto es, si quien interviene como parte en un contrato no es el titular de los datos que ha facilitado como propios para su identificación -como sucede, por ejemplo, en las contrataciones fraudulentas- el tratamiento no puede estimarse lícito en aplicación de la circunstancia del artículo 6.1.b), pues el titular de los datos no es en tal caso parte en el contrato, sino que es ajeno a él. De igual forma, si el poder de representación es insuficiente para celebrar un contrato en nombre del poderdante el tratamiento de sus datos personales no puede reputarse lícito en aplicación del artículo 6.1.b), pues el contrato suscrito por quien no ostenta representación para intervenir en él no produce efectos en la esfera jurídica del representado. En virtud del principio de responsabilidad proactiva (artículo 5.2 RGPD) el responsable está obligado a desplegar la actividad necesaria para cumplir los principios que deben presidir el tratamiento de datos, por lo que aquí interesa el principio de licitud. Y debe de estar también en condiciones de acreditar su cumplimiento. El principio de responsabilidad proactiva se proyecta tanto sobre la diligencia que es exigible al responsable del tratamiento -quien ha de adoptar las medidas técnicas y organizativas necesarias para cumplir los principios que presiden el tratamiento, recogidos en el artículo 5.1 del RGPD- como sobre la carga de la prueba de su cumplimiento. De manera que el responsable que pretenda amparar la licitud de un tratamiento de datos en el apartado b) del artículo 6.1 RGPD deberá actuar diligentemente y verificar que quien interviene en la contratación es también el titular de los datos con los que se ha identificado como parte contratante.(…) la entidad bancaria no obró con la diligencia que como tal entidad se le debe exigir puesto que incluyó en la cuenta corriente a una persona que no estaba suficientemente representada en el poder empleado por el tercero para la apertura de la misma y su inclusión obedeció tan solo a esa posición genérica de comunera o miembro de una comunidad de bienes. En consecuencia, la entidad bancaria con su actuación vulneró el principio de licitud del tratamiento en relación con el artículo 6.1.del RGPD, infracción tipificada en el artículo 83.5.a) del citado RGPD, apreciada por la resolución recurrida.

En cuanto a los principios de **integridad y confidencialidad**, es preciso citar las Sentencias de fechas 8 de febrero y 13 de mayo de 2024, ambas referidas al tratamiento de datos personales derivado del duplicado fraudulento de tarjetas SIM.

La primera es la **Sentencia recaída en el Recurso Núm. 2250/202**, en la que Los hechos sancionados hacen referencia, como se dice en la resolución recurrida, al fraude conocido como "SIM Swapping", *consistente en obtener un duplicado de la tarjeta SIM asociada a una línea de telefonía titularidad de un usuario, con la finalidad de suplantar su identidad para obtener acceso a sus redes sociales, aplicaciones de mensajería instantánea, aplicaciones bancarias o comercio electrónico, con la finalidad de interactuar y realizar operaciones en su nombre, autenticándose mediante un usuario y contraseña previamente arrebatados a ese usuario, así como con la autentificación de doble factor al recibir el SMS de confirmación en su propio terminal móvil donde tendrán insertada la tarjeta SIM duplicada*.

Es decir, lo destacable de esta estafa es que, en una primera fase, el suplantador consigue, de manera fraudulenta, los datos de acceso o las credenciales de la banca online del cliente, pero le falta por conocer el código de verificación, segundo factor de autentificación, para poder ejecutar cualquier operación. En el momento en el que logra la tarjeta SIM duplicada ya tiene también acceso a este segundo factor de autentificación y, por tanto, desde ese momento puede realizar los acos de disposición patrimonial que desee.

La entidad recurrente, alega, en primer término, que la responsabilidad de lo sucedido es de los encargados y, en su caso, subencargado, que dejaron de observar las instrucciones de aquella y trataron los datos para sus propios fines, lo que supone la exoneración del responsable de acuerdo con el artículo 28.10 del RGPD.

La Sala reprocha a la recurrente la aplicación del artículo 24.1 del RGPD, por cuanto el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento, y en segundo término, lo indicado en el artículo 28.1 del RGPD que impone la obligación de que *el responsable del tratamiento elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado*.

De la prueba practicada se concluye que *no ha quedado acreditado que las citadas empresas, como encargadas del tratamiento de la parte actora, hayan determinado fines y medios del tratamiento, ni hayan utilizado los datos de los clientes de aquella para sus propias finalidades, ni han interactuado frente a los interesados ajenos a la estructura y nombre comercial de la sociedad recurrente, sino que han actuado bajo el nombre de la parte actora para el cumplimiento de los fines de estos, utilizando los sistemas de ésta para realizar las operaciones con los clientes. Por lo que, no cabe invocar el art. 28.10 del RGPD para una presunta atribución de responsabilidad a los encargados que, además, implique la exoneración del responsable del tratamiento, es decir, de la recurrente*.

La Sala concluye: *La parte actora como responsable del tratamiento de datos, habida cuenta del resultado de las tres reclamaciones, no había garantizado una seguridad adecuada en el tratamiento de los datos personales, como se deriva del resultado que produjo la suplantación de identidad. Y, por ello, un tercero consiguió acceder a los datos personales de los titulares de las líneas sin que las medidas de seguridad que existían hubieran podido impedirlo.*

Otra prueba de ello, de que las medidas de seguridad en el momento en que se produjeron los hechos no eran las adecuadas, es que, se produjo un cambio en dichas medidas (…)

Por su parte, la **Sentencia recaída en el Recurso Núm. 2336/2021** tiene hechos similares, que hace el siguiente análisis del **principio de culpabilidad** al indicar que:

(…) *como señala la Sentencia del Tribunal Supremo de 18 marzo 2005 – Rec. 7707/2000-, "no podría estimarse cometida una infracción administrativa, si no concurriera el elemento subjetivo de la culpabilidad o lo que es igual, si la conducta típicamente constitutiva de infracción administrativa no fuera imputable a dolo o a culpa". Conforme a ello, es la falta de diligencia de la entidad recurrente, como responsable del tratamiento, a la hora de implementar en origen las medidas de seguridad adecuadas para comprobar que la persona que solicita o activa el duplicado de la tarjeta SIM es realmente el titular de ésta, lo que constituye el elemento de la culpabilidad. Falta de diligencia que en el presente supuesto se desprende de los hechos declarados probados en relación con las nueve reclamaciones pormenorizadamente descritas en los mismos, tantas veces citadas. No podemos olvidar que, para poder efectuar cualquier operación, transferencia o compra no consentida, el ciberdelincuente deberá acceder ilegítimamente a los códigos de verificación asociados a cada una de esas operaciones remitidos por la entidad bancaria a través de SMS y la manera más habitual de hacerlo, es a través de la obtención de un duplicado de la tarjeta SIM. Siendo por dicha obtención de duplicado con insuficientes medidas de seguridad, por la que ha sido sancionada la entidad actora. En cuanto al hecho de que nos encontramos ante el fraude de un tercero, la AEPD no ha extendido la responsabilidad de la entidad demandante más allá de sus obligaciones como responsable del tratamiento, no examinando las actuaciones de terceros intervinientes, como serían los suplantadores o las entidades bancarias*.

Siguiendo con el **principio de integridad y confidencialidad**, pero en un ámbito distinto al de las Sentencias comentadas, destaca la **Sentencia de 13 de septiembre de 2024 recaída en el Recurso Núm. 2187/2021**, referida al envío por correo electrónico de mensajes con datos personales, a varios destinatarios sin utilizar la función de copia oculta. Lo interesante de la resolución es la argumentación sobre los datos revelados, entre los que figuraba el DNI y que la entidad

recurrente sostiene que es un dato público y por tanto desprovisto de la protección que ofrece la normativa de protección de datos.

Dice la Sentencia que el recurrente "*alega que el DNI puede constituir información pública, cuando existen notificaciones en Boletines Oficiales, oposiciones, como es el caso del reclamante cuyo número de DNI aparece, por ejemplo, en la Resolución de 8 de julio de 2015 de la Dirección General de la Policía, por la que se hace pública la lista de admitidos y excluidos de la oposición de ingreso en la escala básica, categoría de policía, del Cuerpo Nacional de Policía, o en la Resolución de 8 de enero de 2008 de la Jefatura de Enseñanza de la Guardia Civil por la que se hace pública la lista de aspirantes excluidos definitivos de la convocatoria de las pruebas selectivas para el ingreso en los centros docentes de formación para incorporación a la Escala de Cabos y Guardias de la Guardia Civil*".

Contesta la Sala en los siguientes términos: *la Ley Orgánica 3/2018, en su Disposición Adicional séptima referente a la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos y a las notificaciones infructuosas, no permite publicar el nombre y apellidos de los afectados unido a su número completo de DNI. El hecho de que el número del DNI aparezca publicado en el BOE en relación con determinados procesos selectivos y en fechas anteriores a la citada Ley Orgánica 3/2018 y con una finalidad determinada, no significa que su tratamiento y puesta en conocimiento respecto del otro empleado de UST Global sea legítimo, como pretende la actora, sino que debemos que ir al art 6, apartado 1 del RGPD, que prevé una lista exhaustiva de los casos en los que un tratamiento de datos personales puede considerarse lícito. Así pues, para poder ser considerado legítimo, el tratamiento de datos personales debe estar comprendido en alguno de los casos contemplados en esa disposición*.

Referida a los **principios de licitud y minimización**, hay que hacer referencia a la **Sentencia de 18 de marzo de 2024 recaída en el Recurso Núm. 710/2022**, en el que los hechos objeto de análisis se concretan en la denuncia de un afectado y su esposa referente al proceso de registro en un establecimiento hotelero en el que observan como "*sus pasaportes fueron escaneados y se guardaron digitalmente sus copias2*, y posteriormente observan que en la Tablet de los camareros aparecía sus fotografías y que el personal del hotel tenía acceso a sus datos.

La entidad recurrente alegaba que *la imagen con la foto del cliente se utiliza para facilitar al personal del hotel la identificación del cliente que está haciendo uso de la tarjeta del crédito o habitación (en el momento de realizar un consumo, el cliente facilita esa tarjeta al empleado, quien, al pasarla para realizar el cargo, puede comprobar la fotografía), así como para controlar el acceso al establecimiento*.

Por tanto, el tratamiento objeto de análisis era la incorporación de los datos del cliente (número de habitación y de la reserva, número de personas y fecha de salida; nombre y apellidos de la persona, régimen, tipo de VIP y número de visitas, además de la fotografía del cliente), a los dispositivos empleados por el personal de servicio del hotel que se utiliza para verificar la identidad del cliente cuando realizan consumos en el hotel.

La Sala aborda la posible aplicación del interés legítimo como base legitimadora del tratamiento, articulo 6.1 f) RGPD, para lo que se requiere un juicio de ponderación que haga prevalecer el interés legítimo del responsable o de un tercero, sobre los intereses o derechos y libertades del interesado, todo ello sin olvidar la sujeción al principio de minimización, (artículo 5.1. c)), que informa la materia y conforme al cual "Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)", y así lo ha declarado el TJUE en su sentencia de 1 de agosto de 2022, C-184/20.

Sostiene el tribunal que el juicio de ponderación *no se ha llevado a cabo por parte de la demandante adecuadamente y de forma ajustada a lo establecido. Ello es así porque no se informó debidamente al titular de los datos de la finalidad del tratamiento de la fotografía, como se recoge en el hecho probado Sexto, pues la "Política de privacidad del establecimiento hotelero", en la que se informa del tratamiento de la foto y su finalidad de controlar los cargos de los consumos realizados en el establecimiento, no está fechada y se presentó*

con el escrito de alegaciones a la propuesta de resolución fechado el 12 de diciembre de 2021; en la documentación presentada por la demandante en el período probatorio del procedimiento sancionador no figura ninguna mención concreta al respecto. En esas condiciones no resultaba posible realizar el juicio de ponderación entre el interés legítimo alegado por el establecimiento para controlar los consumos y evitar el fraude y los derechos del denunciante a la intimidad y a la protección de datos personales, para determinar si concurrían las restantes condiciones inherentes a ese principio, es decir, la pertinencia de las medidas y su adecuación, considerando las posibles alternativas menos intrusivas y valorándolas en relación con la finalidad perseguida; más bien el denunciante se opuso al escaneo de su pasaporte y sólo fue consciente de que su foto aparecía en el dispositivo de los empleados al ir a pagar una consumición, lo que prueba que ni había prestado el consentimiento, ni había sido informado.

En conclusión, el tratamiento, no consentido por el titular de los datos, no estaba amparado por el artículo 6.1.f) RGPD y, por tanto, no puede considerarse lícito.

En relación con la **seguridad del tratamiento y la gestión de las violaciones de datos**, ha y que citar la **Sentencia de 4 de julio de 2024 recaída en el Recurso Núm. 382/2022**

Respecto de la vulneración del artículo 32 del RGPD, la sala recuerda lo indicado en los informes -aportados por la recurrente- en los que se basa la AEPD para fundamentar la sanción. En el primero de ellos *se pone de manifiesto las numerosas vulnerabilidades graves: El acceso a unas 4000 tarjetas de crédito con la finalidad de cometer fraude; el atacante hubiera recopilado como mínimo 488847 tarjetas de crédito únicas; que visualizara y archivara en SNMIDSRVPRD02 al menos 2651 números de tarjeta únicos, CVVs, fechas de vencimiento y nombres de titular de la tarjeta, y el número aproximado de registros afectados fueran 1.500.000, etc*.

Y la mencionada empresa, proponía una serie de recomendaciones: Revisar la política de auditoría y retención y aplicarla uniformemente en todo el entorno y valorar la posibilidad de centralizar la recopilación de registros en una plataforma exclusiva, como un producto de Gestión de Incidencias e Información de Seguridad; que aunque no ha sido posible determinar exactamente la fuente de la infección de los sistemas en alcance, una de las hipótesis más probables es que los sistemas se vieran infectados por una segregación insuficiente entre el entorno de oficina y el entorno de producción gestionando los datos de las tarjetas de pago; bloquear y supervisar el tráfico de salida a direcciones IP externas sospechosas y se observaron diversos sistemas con un funcionamiento más largo de un año, por lo que los sistemas operativos no contaban con parches para un periodo tan largo.

Y en el segundo informe consta *que se habían identificado pruebas concluyentes de la violación de seguridad; la identificación de 2,7 millones de tarjetas que habían sido extraídos de los sistemas de bases de datos consiguiendo el atacante utilizar herramientas de descifrado presentes en los sistemas; que el acceso tuvo su origen en sistemas inseguros disponibles a través de internet, identificando varios dispositivos que no se habían parcheado con regularidad; un resumen de las posibles causas que habrían motivado el ataque (que el código del atacante consiguió conectarse directamente el servidor (…); que los sistemas comprometidos no habían sido parcheados durante más de 6 meses; que la entrada del atacante en los sistemas a través de servidores que tenían acceso a los servidores(…); la existencia de indicadores que podrían haber advertido de la violación antes del momento de su detección); la existencia de pruebas de violación del entorno de datos de los titulares de las tarjetas; que el ataque comenzó al accederse al entorno (…) desde un servidor no adecuadamente segmentado en el citado ámbito; que el atacante tenía una conexión sistemática con un host externo y que debido a la falta de registro, no se pudieron identificar todas las transmisiones de datos realizadas fuera de la red; la posible exposición de determinados tipos de datos (nombre del titular de tarjeta, dirección de titular de tarjeta, fecha de vencimiento)*".

Tal y como considera la AEPD, entiende la Sala que estas conclusiones son suficientes como para apreciar la existencia de la infracción del artículo 32.1 del RGPD: *conforme a lo expuesto, las medidas de seguridad técnicas y organizativas implantadas por la parte demandante no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los*

datos de los clientes, apreciándose la existencia de la infracción del art. 32.1 del RGPD.

En cuanto a la infracción del artículo 33 del RGPD, la Sala considera que *hay que tener en cuenta como fecha en que tuvo conocimiento la parte recurrente de la violación de la seguridad de los datos personales, el 16 de octubre de 2018, y, como se dice en la resolución sancionadora, la notificación, "se realizó de manera extemporánea 41 días después de que fuera conocida infringiendo claramente lo dispuesto en el artículo 33 del RGPD…".*

Por tanto, la notificación la violación de seguridad de los datos personales, se produjo fuera del plazo de las 72 horas previsto en el art. 33 del RGPD.

Por su parte, la **Sentencia de 1 de marzo de 2024, recaída en el Recurso núm. 1757/2021** sobre la sanción impuesta a una entidad del sector energético por vulneración de los artículos 25 y 13 del RGPD. por falta de una efectiva implementación de medidas técnicas y organizativas por parte la entidad para eliminar los riesgos que genera la contratación de servicios y para la obtención de consentimiento para otras finalidades, cuando se actúa a través de representante.

La recurrente entiende que no existe ninguna previsión ni en el Código Civil ni en la normativa de protección de datos que exija que el apoderamiento dirigido a prestar el consentimiento sobre un tratamiento de datos accesorio al mandato principal deba estar revestido de una formalidad especial o haya de ser objeto de acreditación distinta de la general, ni tampoco existe disposición alguna que imponga al tercero el deber de llevar a cabo una comprobación sobre cuál es el alcance del apoderamiento con el que actúa el representante.

La Sala entiende en síntesis que, atendiendo a los diferentes canales de venta o contratación de servicios, en unos si se solicita la acreditación de la representación, mientras que en otros no se hace.

Sobre esta premisa, la sentencia indica que : "*la medida en que no se ha implantado un procedimiento que permita acreditar la representación de quien efectúa una contratación en nombre de un tercero, se pueden generar diversos riesgos, tales como el tratamiento de datos del representado sin legitimación, la suplantación de identidad o los perjuicios económicos o de otro tipo que se puedan ocasionar al interesado como consecuencia del cambio de compañía suministradora del servicio o el cambio de la titularidad del contrato o de la modalidad de contrato con la compañía suministradora, sin que el interesado haya consentido dichos cambios. (…) al no haberse implementado un procedimiento que permita acreditar que el representante disponía de la autorización del representado para consentir el tratamiento de datos del representado con fines publicitarios a que se ha hecho referencia, se produce el riesgo de tratamiento de datos del representado sin legitimación, quedando expuesto a la recepción de publicidad incluso después de finalizada la relación contractual. Riesgo que se incrementa en el canal fuerzas de venta externas, dado que no se envía el contrato al representado, sino que se da copia al representante al que se responsabiliza de informar al representado.*"

Sobre el riesgo de suplantación de identidad, la Sentencia recoge que: *pese a que el contrato de mandato no está sujeto en el Código Civil a un requisito formal para su eficacia, atendiendo a los riesgos para los derechos y libertades de las personas físicas, uno de los cuales en este caso es claramente la suplantación de identidad (Art. 28.2.a) de la LOPDGDD) que la demandante admite que existe, pero con una baja incidencia, se establece por el RGPD un plus imponiendo la necesidad de medidas adecuadas.*

Por ello, resulta preciso que el responsable del tratamiento se asegure de la representación, no es un requisito impuesto al representante, sino que es una obligación prescrita en el art. 25 del RGPD propia del responsable del tratamiento.

La AEPD no entra a valorar la validez y eficacia de la representación, ni que el apoderamiento no sea un medio valido para contratar en nombre de otra persona, previsión que queda fuera de su ámbito competencial, sino la necesidad de implementar medidas adecuadas que aseguren que tal representación existe atendiendo los riesgos que entraña el tratamiento de dichos datos.

La Sala concluye que: *se impone al responsable del tratamiento que verifique la exactitud de los datos del interesado a través de la implementación de las medidas adecuadas cuando se efectúe una*

contratación. Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento, y a ello obedece la exigencia de documentación identificativa, como viene reiterando la Sala entre otras en Sentencias de 3 de octubre 2013 (Rec. 54/2012), 21 de noviembre 2014 (Rec. 45/2014) etc.

Obligación que es trasladable a los supuestos de representación, en que no solo es necesario comprobar los datos del interesado sino también los del representante que está actuando en nombre del representante y su efectiva representación.

Respecto de la infracción del principio de transparencia y el derecho a la información, la Sala confirma el criterio de la Agencia por cuanto, durante el proceso de contratación telefónica y durante el proceso de contratación por fuerzas de ventas externas, no si da la misma información, y se ofrece información errónea en cuanto al responsable del tratamiento, "*el hecho de que en el contrato se especifique la empresa con la que se contrata, implica que el interesado conoce la entidad con la que ha contratado los servicios, pero no el responsable de los distintos tratamientos de datos que puedan efectuarse, por cuanto en las condiciones generales de la contratación se indica que dichos datos "serán tratados por EDP Comercializadora SAU, con domicilio en (…) y por EDP Energía SAU con domicilio en (…) en su calidad de Responsables del tratamiento (…)", a lo que se añade la referencia genérica EDP en el resto de la información facilitada. De esta forma, ante esa imprecisión en cuanto al responsable del tratamiento, el cliente que haya contratado únicamente un servicio con una de las dos entidades no puede saber si sus datos van a ser tratados por la entidad con la que ha contratado o por las dos.*

Y en estos casos, no se informa correctamente al interesado sobre quien es el responsable de los tratamientos, y no puede sostenerse que la información se ofrece de forma concreta y clara para el interesado."

En el ámbito del **tratamiento de imágenes mediante dispositivos de videovigilancia**, procede citar en primer lugar la **Sentencia de 28 de noviembre de 2024 recaída en el Recurso Núm. 2172/2021** interpuesta por un particular contra la resolución sancionadora de la AEPD por vulneración de los principios de minimización y de limitación del plazo de conservación (artículo 5.1 c) y d) del RGPD. Comienza la resolución recordando la doctrina sobre la imagen como dato personal y la consideración de tratamiento en lo referente a la captación y grabación: *Esta Sala ha declarado en múltiples ocasiones (Sentencias de 29 de mayo de 2015 -recurso nº. 94/2014-, de 19 de diciembre de 2018 -recurso nº. 286/2017 y de 25 de mayo de 2023 -recurso nº. 574-2022, entre otras), que la imagen de una persona grabada por una cámara constituye un dato personal, en la medida en que permite identificar a la persona afectada, como señala la Sentencia del Tribunal de Justicia de la Unión Europea de 11 de diciembre de 2014 (asunto C- 212/13). Y, asimismo, constituye doctrina consolidada y reiterada que la captación y grabación de las imágenes de personas recogidas por las cámaras de videovigilancia constituye un tratamiento de datos de carácter personal, sujeto a la normativa de protección de datos y, en concreto, a la exigencia de consentimiento inequívoco del afectado del artículo y al principio de proporcionalidad, esencial en esta materia.* (…).

También cita el artículo 22 de la LOPDGDD como supuesto legitimador que delimita los requisitos de pertinencia, utilidad y proporcionalidad, y su relación con la normativa de Seguridad Privada, en concreto con la Ley 5/2014 de 14 de abril.

Por lo que se refiere a las cámaras a través de las cuales se graba la vía pública, el hecho de que un sistema de videovigilancia haya podido ser instalado conforme a la normativa de seguridad, no autoriza a realizar grabaciones de imágenes en la vía pública más allá de lo que resulta idóneo, adecuado y proporcional, siendo lo esencial si a través de ellas es susceptible de captar o no a personas que se encuentran en la vía pública, en cuyo caso tal tratamiento ha de respetar el principio de proporcionalidad, esencial en esta materia.

La Sala concluye que *cabe apreciar la existencia de la infracción que estamos analizando, de conformidad con las pruebas que consta en el expediente administrativo, y de las manifestaciones del recu-*

rrente, en las que se reconoce la existencia de dos cámaras de videovigilancia "están instalados en vivienda unifamiliar" con fines de protección de la vivienda frente a intrusos, y, debemos añadir, que se encuentran orientados hacia un camino donde transitan terceros. No resulta valida la exculpación que hace el recurrente de que dicho camino es privado, ya que lo cierto es que existe una controversia con el Ayuntamiento de Santiago de Compostela, tramitándose el recurso correspondiente en el Juzgado de lo Contencioso-Administrativo Número 1 de Santiago de Compostela - procedimiento ordinario. 345/2020-.

Por otro lado, dicha instalación de las cámaras hay que considerarla excesiva, pues el mero vallado del terreno es suficiente para la protección de la zona, pudiendo las cámaras instaladas realizar un "tratamiento de datos" sobre un terreno sobre cuya naturaleza no existe pronunciamiento judicial firme alguno.

También se estima la comisión de la infracción del articulo 5.1 e) del RGPD referida al principio de limitación del plazo de conservación, en relación con el artículo 22.3 de la LOPDGDD, que limita, con carácter general el plazo de conservación máximo de un mes desde la captación, teniendo en cuenta que el propio recurrente reconoce que conserva las imágenes durante dos meses.

En segundo lugar, procede citar la **Sentencia de 20 de septiembre de 2023 recaída en el Recurso Núm. 2201/2021** y notificada a la Agencia en el ejercicio 2024, que es similar a la anteriormente citada, pero merece cita por la solución adoptada.

La Sentencia confirma la resolución de la Agencia de inadmisión y desestima el recurso interpuesto, en esencia, por falta de motivación.

No obstante lo relevante de la misma son precisamente los motivos por los que la Agencia no estimó la existencia de infracción que hace suyos el tribunal: *la denuncia parte de la grabación realizada por una cámara de videovigilancia colocada en una propiedad particular que grabó unas imágenes presentadas por el dueño de la finca ante la policía como prueba de unos daños causados en el acceso a su propiedad, por los que se siguió un procedimiento inmediato por delito leve ante el Juzgado de Instrucción nº 3, que derivó en una condena por delito leve contra el aquí demandante por delito leve de coacciones en concurso medial con un delito leve de daños, en sentencia de 18 de enero de 2021, confirmada por la Audiencia Provincial de Barcelona el 21 de abril del mismo año. La captación de imágenes por videovigilancia, por tanto, parece limitada al mínimo del espacio público necesario para captar la entrada en la finca, en cuya puerta de acceso se produjeron los daños, lo que no infringe lo establecido en el artículo 22.1 y 2 de la Ley de Protección de Datos que permite en términos generales el tratamiento de imágenes con la finalidad de preservar la seguridad de personas y bienes así como sus instalaciones; no consta la existencia de otras grabaciones con datos personales o imágenes de personas captadas en la vía pública y sí únicamente la del denunciado utilizada en el juicio; tampoco es relevante el hecho de que se comunicara o no a la AEPD la colocación de la videocámara, que se instaló precisamente ante la repetición de daños causados en la cerradura que dificultaban el acceso a la vivienda, pues conforme al Reglamento General de Protección de Datos y la L.O. de Protección de Datos de 2018, no se requiere autorización por parte de la Agencia ni se exige la inscripción de los ficheros de datos personales en la AEPD; la existencia de un cartel informativo, que aparece en algunas de las fotos aportadas y no en otras es irrelevante pues la cámara, situada en el interior de la finca estaba enfocada hacia la puerta. Además, conforme al artículo 6.1.e) RGPD y 8 LOPDGDD el tratamiento es lícito cuando, como en este caso, la grabación se aportó con una denuncia por daños ante la policía y posteriormente a la jurisdicción penal que, en el ejercicio de las competencias legales atribuidas, la utilizó como prueba en un juicio al que el denunciado, aquí demandante, decidió no acudir, y cuya validez no fue cuestionada*.

Destaca como novedosa, la **Sentencia de 5 de diciembre de 2023 recaída en el Recurso Núm. 1423/2021** (notificada a esta Agencia ya en el ejercicio 2024 razón por la que se incluye en la presente memoria,) dado que la materia que aborda es la **denegación de aprobación por la AEPD de un Código de Conducta**, en este caso el Código de conducta del Sector Infomediario de Protección de Datos de Carácter Personal" cuyo promotor es la Asociación Multisectorial de la Información (ASEDIE).

La AEPD deniega la aprobación del repetido código de conducta, en base a tres motivos esenciales, que se recogen fundamento de derecho IX de la resolución, y que son:

De un lado porque debería haberse acompañado toda la documentación justificativa a la que se ha ido haciendo referencia a lo largo de la tramitación (Memoria y, en su caso, Análisis de Riesgos y Estudio de Impacto de Protección de Datos, cuando sea necesario para justificar la adecuación del código a la normativa aplicable).

Además, porque la regulación de los sistemas de información crediticia con datos relativos al cumplimiento de obligaciones dinerarias, financieras o de crédito y de los sistemas de información sobre solvencia patrimonial con datos obtenidos de fuentes públicas o que el interesado haya hecho manifestantes públicos, contenida en las secciones 2ª y 3ª del Anexo II, que deberían suprimirse.

Y en tercer lugar porque debería procederse a una profunda revisión del resto del código para su completa adecuación a los principios y normas contenidos en el RGPD y la LOPDGDD".

La recurrente pretende la anulación parcial de la Resolución de la AEPD, es decir una parte de las consideraciones, esto es la parte controvertida en la que basa la denegación, y no la parte dispositiva de la misma.

La falta de antecedentes jurisprudenciales en la materia, novedosa en el ámbito de la jurisdicción contencioso-administrativa, considera la Sala aplicable la doctrina de la Sala de lo Social del Tribunal Supremo, que se invoca por el Abogado del Estado en la contestación, y que se recoge, entre otras, en las SSTS de 18 de julio de 2002 (Rec. 1289/2001) de 15 de septiembre de 2015 (Rec. 252/2014) y de 27 de febrero de 2017 (Rec. 12072016) , Jurisprudencia que se resume en la STSJ (Madrid), de 9 de octubre de 2023 (Rec. 441/2023), entre las más recientes, en los siguientes términos :

"Como señalaba la STS de 14-05-2000 (Casación 95/2008), "*la doctrina científica y judicial mayoritaria considera el derecho de acción, como el derecho a acudir a los órganos judiciales y obtener en el proceso un pronunciamiento de fondo sobre los derechos sustantivos de los que el accionante afirma ser titular o tener un interés legítimo respecto de ellos. Ahora bien, ese pronunciamiento de fondo puede no llegar producirse si se alega por la contraparte la denominada, en la praxis, excepción de " falta de acción" y se prueba la inexistencia de la titularidad o de la posición de interés legítimo que en relación con el derecho sustantivo esgrime el accionante para recabar su tutela* (…)".

La resolución de la AEPD impugnada contiene un solo y único pronunciamiento que no se impugna por la entidad actora, sino que lo que tal recurrente pretende es su anulación parcial, y de una parte de los motivos de la resolución, no de la parte dispositiva de la misma, por lo que ASEDIE carece de acción, en cuanto derecho a acudir a este tribunal recabando la tutela de un derecho e interés, dada la ausencia de dicho interés real y en definitiva de una auténtica controversia jurídica. Por otra parte, y esto es asimismo relevante, resulta que si se dictara un eventual pronunciamiento estimatorio de la pretensión de la demanda, el Código de Conducta seguiría sin poder ser aprobado, ya que el resto de los defectos apreciados por la AEPD (la falta de memoria y análisis de riesgos y Estudio de Impacto, y , sobre todo la profunda revisión de dicho Código a que obliga la Resolución combatida para adecuarlo a la normativa de protección de datos), que no han sido impugnados por ASEDIE en el presente recurso contencioso-administrativo, no se verían alterados por tal eventual estimación, lo que conduciría a una situación anómala y que asimismo evidencia la inexistencia de una autentica litis o controversia en la pretensión ejercitada por dicha entidad actora, por lo que el recurso ha de ser desestimado.

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 éstas últimas hay que citar en primer lugar la **Sentencia de 7 de marzo de 2024 recaída en el Recurso Núm. 2282/2021** referida al tratamiento de datos con finalidades de mercadotecnia directa tras haber ejercido el **derecho de oposición** (artículo 21 RGPD) mediante el envío de correos electrónicos, y cuyo tratamiento también está afectado por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y de Comercio Electrónico. (LSSI).

La Sentencia tras concretar el régimen jurídico aplicable señala que la recurrente ha sido sancionada al no acreditarse que el denunciante haya otorgado su consentimiento para la recepción de correos electrónicos con publicidad de la parte actora. Y entra a rebatir las alegaciones de la recurrente sobre la no consideración de dato personal de la dirección de correo electrónico destinataria de los envíos publicitarios.

Dice la recurrente que el supuesto que nos ocupa, (…) *remitió las comunicaciones comerciales que traen causa del presente contencioso a la dirección de correo electrónico profesional dpd@(xxxxx).es, gestionada por el denunciante. Debido a la configuración alfanumérica de esta dirección de correo electrónico, sin incluir referencia alguna a nombres o apellidos, sino constituyendo una denominación genérica, abstracta y correspondiente a un área de la entidad titular del dominio, dicha información no puede ser considerada como dato personal*.

La Sala recuerda la doctrina sobre la consideración de dato personal aplicable al caso: Como dijimos en la Sentencia de 23 de julio de 2019 -recurso nº. 146/2018-: "*Se trata, por tanto, de un concepto muy amplio que incluye no solo el nombre, apellidos, dirección, número de DNI y determinados datos relativos a la profesión de la persona, así como a su identidad física, psíquica y genética, sino también el número de teléfono, incluso sin aparecer directamente asociado a una persona, siempre que a través de él se pueda identificar a su titular (SAN de 26 de enero de 2005 (Rec. 1258/2002), así como la dirección de correo electrónico, aunque en la composición de la leyenda inicial de dicha dirección no aparezca el nombre y apellidos del titular (SAN 22 de febrero de 2006 (Rec. 911/03). En la STC 14/2003, de 30 de enero, por otra parte, también se conceptúa como dato de carácter personal la imagen de una persona. Y la SAN de 1 de septiembre de 2011, Rec. 625/2009, igualmente ha considerado como tal dato personal la dirección IP*".

Por lo que, en principio, la dirección de correo electrónico es considerada a todos los efectos como un dato de carácter personal. Y, por otro lado, cuando la dirección de correo electrónico de una empresa, como en presente supuesto (…@XXXX.es), es utilizado por un solo empleado, pudiéndose identificar directa o indirectamente con el nombre, con determinados dígitos o con el cargo que ocupa, como es el caso, <<delgado de protección de datos>> (dpd@...), se considera dato personal a todos los efectos."

En segundo término, se valora -y se desestima- las alegaciones de la actora referidas a que los envíos los realizaron entidades que actuaban como encargado del tratamiento incumpliendo las instrucciones del recurrente y, por tanto, siendo utilizados para los fines propios de estas. La Sentencia contradice dicho argumento sobre la base los contratos y el contenido de los correos comerciales enviados: *de conformidad con el citado el art. 28.10 del RGPD, Cablanol S.L. podría considerarse responsable del tratamiento si hubiera actuado, "(…) al margen o en contra de las instrucciones legales del responsable (…)". Por el contrario, ha quedado acreditado que Cablanol S.L. envió varios correos electrónicos publicitarios haciendo referencia a determinadas ofertas de la operadora VODAFONE, con frases publicitarias como: "ACTUALIZA LAS COMUNICACIONES DE TU EMPRESA CON VODAFONE" o "(…) Vente a VODAFONE. Ahora tus líneas y centralita con grandes descuentos (…)", Por tanto, Cablanol S.L. realizó el envío de los correos electrónicos publicitarios de acuerdo con las directrices encomendadas por la operadora Vodafone, estableciendo relaciones con los destinatarios de los correos electrónicos, por mandato de la operadora y promocionando servicios de ésta. Por tanto, queda acreditado que, el responsable último de los hechos acaecidos es la operadora Vodafone*.

También en relación con los derechos, la **Sentencia de 29 de octubre de 2024 recaída en el Recurso Núm. 1061/2022**, que, si bien aborda el tratamiento por sistemas de videovigilancia en una cadena de supermercados, lo esencial es cómo se gestiona la **solicitud del derecho de acceso** realizado por un particular. Los hechos se resumen en que una persona sufre una caída en el establecimiento el día 2/10/2020 y el día 18 del mismo mes ejerció el derecho de acceso frente a las imágenes captadas el día del accidente. El 4 de diciembre se reitera la petición y la entidad sancionada manifiesta el día 9 de ese mes que ni consta solicitud alguna y que en cualquier caso las imágenes han sido borradas.

Se alega por la recurrente que todo se debió a un error humano en la gestión de la solicitud del derecho de acceso.

La Sala confirma la sanción por vulneración del artículo 15 del RGPD al indicar que El artículo 15 regula el derecho de acceso en los siguientes términos: "El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales" y a la información que desarrolla en los apartados siguientes estando obligado el responsable del tratamiento, a facilitar una copia de tales datos objeto de tratamiento, que no ha de afectar negativamente a los derechos y libertades de terceros.

En este caso, como reconoce la resolución la empresa disponía de protocolos para ejercitar el derecho de acceso; el sistema funcionó correctamente pero fue interrumpido por el descuido de un empleado (gerente de tramitación) al que el sistema había asignado la solicitud, que no la trasladó al delegado de protección de datos para continuar la tramitación, como se reconoce en la demanda (Hecho Tercero), de modo que éste no tuvo conocimiento de la misma hasta transcurridos más de dos meses desde el día del accidente y su posible grabación por las cámaras de videovigilancia, indicando que la grabación había sido eliminada, por lo que no podía atender lo solicitado.

En estas condiciones resulta claro que la solicitud de acceso no fue atendida debidamente y en plazo por el descuido de un empleado de la empresa, descuido sobre el que no se ha aportado dato alguno que permita calificarlo como involuntario, como pretende la demandante para eliminar la concurrencia del elemento culpabilístico de la infracción y lo prueba el hecho de que, además del acuerdo con la reclamante para indemnizarla se adoptaron a nivel interno medidas disciplinarias, entre otras mencionadas también en el mismo hecho tercero de la demanda. Así la demandante infringió el artículo 15 en relación con el 83.5 b) RGPD, como apreció la resolución impugnada por lo que procede en este punto confirmarla.

Por el contrario, la Sala no aprecia la vulneración del artículo 6 del RGPD que también se apreciaba en la resolución recurrida por no compartir el criterio de la Agencia referido a que el borrado de los datos se hizo sin base jurídica alguna y por tanto incumpliendo el citado precepto. Considera el tribunal que la entidad eliminó correctamente los datos porque no fue conocedora de la solicitud del derecho de acceso y actuó conforme a la Instrucción 1/2006 y al artículo 22.3 de la LOPDGDD.

Por su parte, la **Sentencia de 21 de mayo de 2024 recaída en el Recurso Núm. 538/2020** aborda el **derecho de acceso sobre datos que previamente habían sido bloqueados**. Tras un procedimiento de Tutela de Derechos (actualmente previsto en el artículo 64.1 de la LOPDGDD) la Agencia requiere a la recurrente *para que o se atendiese el derecho de acceso o se denegase de manera motivada indicando las causas. Ante esta resolución, la actora respondió y en su contestación se especifica que se había procedido al bloqueo conforme al art. 32, y no podía dar ningún dato. En definitiva, Telefónica da respuesta u ofrece respuesta de las razones por las que no puede facilitar el derecho de acceso a la información, y se podrá considerar que es una respuesta escueta, pero da oportuno cumplimiento a la resolución de la Agencia Española de Protección de Datos, por lo que la solicitud de acceso ha sido contestada refiriendo que los datos que se mencionaban no podían facilitarse al encontrarse bloqueados en virtud del art. 32 LO 3/2018, por lo que al dar respuesta de las circunstancias que impedían el cumplimiento del derecho de acceso se está dando respuesta a la exigencia de la resolución de la Agencia Española de Protección de Datos de 4 junio 2019 por lo que no existe infracción del art. 58.2 RGPD*.

Siguiendo con las resoluciones relativas al ejercicio de los derechos, el siguiente bloque aborda el denominado derecho de supresión referido a los resultados de búsquedas en internet, también denominado **derecho al olvido** cuya regulación se encuentra principalmente en el artículo 17 del RGPD y articulo 93 de la LOPDGDD.

Procede citar la **Sentencia de 6 de febrero de 2024 recaída en el Recurso Núm. 2301/2021** interpuesto frente a la Resolución de la Agencia en el que desestimaba el ejercicio del derecho de supresión frente al buscador Google.

El recurrente solicita la eliminación de varios enlaces a páginas web realizados a partir de distintas combinaciones de su nombre y apellidos y con los términos de búsqueda "el hombre que

mató a (XXXX), asesino de (XXXX)". En defensa de su pretensión alega que *fue condenado por homicidio hace más de trece años y, a pesar de que no cometió ningún delito sexual sobre la víctima, distintos medios de comunicación afirmaron que el demandante también cometió un delito de violación y agresión sexual, después de que la víctima se negara a mantener relaciones sexuales; tales datos son inexactos y erróneos y no existe razón alguna para su divulgación a terceros, como se deduce de los hechos probados de la sentencia penal.*

Dice la Sala: *El demandante, que ejercita el derecho de supresión, fue condenado a una pena de 12 años de prisión por un delito de homicidio que tuvo una especial repercusión por las circunstancias del hecho y el momento en que se produjo y sigue siendo objeto de atención de los medios de comunicación que, en ocasiones, lo han asociado con otros hechos castigados como delitos contra la libertad sexual de las víctimas ocurridos en la misma localidad durante la celebración de la fiesta del Patrón, hechos que causan una particular repugnancia en la sociedad y que pueden ser considerados como de interés general; no se trata, pues, de una información "manifiestamente inexacta", sino que trata del hecho por el que fue condenado que asocia con otros en que las víctimas fueron también mujeres. La supresión que pide no es la de la totalidad de los enlaces, sino la de los que se refieren al hecho mencionado, de gran repercusión en su momento y más allá. En esas condiciones, es claro que debe prevalecer el derecho a la libertad de información, pues el demandante ni en este procedimiento, ni ante la Agencia, ha presentado prueba alguna sobre la inexactitud manifiesta de la información contenida en los enlaces; además, no ha transcurrido un tiempo excesivo entre la fecha de los enlaces, que se refieren no sólo al hecho delictivo y a las circunstancias en que se produjo, sino a las vicisitudes en el cumplimiento de la condena, y la del ejercicio de su derecho al olvido, por lo que tampoco puede decirse que la información haya quedado obsoleta.*

En definitiva el demandante no ha probado la inexactitud manifiesta de la información, centrada en el delito de homicidio declarado en la sentencia penal y el hecho de que en esa misma información se realicen juicios de valor mencionando otros hechos sucedidos en la misma localidad de agresión sexual contra mujeres ocurridas en esas fiestas, no convierte en inexacta la información principal.(…) las especiales circunstancias del caso reflejadas en la sentencia de la Sala Segunda del Tribunal Supremo, justifican la consideración de la información y su difusión de un gran interés para el público, por lo que debe primar el derecho a recibir libremente información y a la libertad se opinión, frente a la protección de los datos personales.(…) Por otra parte, la supresión de enlaces obtenidos a partir de una búsqueda con palabras distintas a las del nombre y apellidos del interesado, que son sus más característicos datos de identidad como persona física, no está comprendida en el ámbito del artículo 17 RGPD ya que términos como "el asesino de (XXXXX)" o "el hombre que mató a (XXXX)", no son datos personales del demandante aunque puedan conducir a resultados sobre los hechos que le conciernen, como también podrían obtenerse tales resultados utilizando otros muchos otros términos de búsqueda; la sentencia del Tribunal Supremo de 17 de noviembre de 2020, R. 6531/19, citada en la demanda para apoyar esta alegación, contempla un supuesto de hecho diferente (búsqueda a partir del nombre y apellidos o sólo de los apellidos) y llega a la conclusión de que no resulta coherente"…reconocer el derecho al olvido cuando la búsqueda se efectúe a partir del nombre (completo) de una persona y negarlo cuando se efectúa sólo a partir de los dos apellidos de esa persona" , lo que no guarda relación con la búsqueda a partir de términos o expresiones diferentes del nombre y los apellidos.

También el artículo 93. 1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, exige que se trate de una "búsqueda a partir de su nombre" con lo que no están incluidos resultados que conduzcan a información sobre esa persona a partir de la utilización de otros términos, ninguno de las cuales incluye el nombre ni los apellidos de quien ejercita el derecho(…)los enlaces cuyo bloqueo se solicita están amparados por el derecho fundamental a la libertad de expresión del artículo 20 de la Constitución, que comprende, como ya se ha dicho, la crítica de la conducta de otro, aun cuando la misma sea desabrida y pueda molestar, inquietar o disgustar a quien se dirige, pues así lo requiere el pluralismo, la tolerancia y el espíritu de apertura de la sociedad democrática. Libertad de expresión a cuyo ejercicio, como igualmente se ha indicado y reitera el Tribunal Constitucional, no es aplicable el límite interno de veracidad que si es aplicable

a la libertad de información. En consecuencia, en vista de las concretas circunstancias del caso, debe prevalecer el interés público y de los internautas, en el marco de la libertad de expresión.

En cuanto a la jurisprudencia del Tribunal Supremo:

Destaca la **Sentencia de 11 de noviembre de 2024, núm. 1792/2024 que resuelve el Recurso de Casación núm. 2960/2023**, interpuesto por la Agencia Española de Protección de Datos, frente a la Sentencia de la Audiencia Nacional de 23/12/2022 que anula las sanciones impuestas a una entidad financiera. El sentido de la Sentencia es favorable a la recurrente fijando la siguiente doctrina casacional:

La Agencia Española de Protección de Datos, en la incoación, tramitación y resolución de un procedimiento sancionador, puede abordar cuestiones fácticas y jurídicas conexas o relacionadas con los hechos y argumentos recogidos en la reclamación que da origen al procedimiento. Y, más específicamente, en el curso de un procedimiento sancionador iniciado a raíz de una o varias reclamaciones en materia de protección de datos personales, cuando se aprecie que las infracciones singulares denunciadas tienen sus origen común en un documento o instrumento de alcance general que define la política de la entidad en materia de protección de datos, la AEPD puede, y aún debe, hacer objeto del procedimiento sancionador a ese mismo documento que alberga la política de privacidad de la entidad responsable, a fin de examinarlo, detectar sus posibles carencias o deficiencias, y adoptar, en consecuencia, las medidas que resulten necesarias en el seno del propio procedimiento sancionador; en el bien entendido de que de todo ello habrá de darse conocimiento al sujeto del expediente, de manera que durante la tramitación del procedimiento pueda este tener ocasión de formular alegaciones y, en su caso, proponer pruebas, sin que en ningún caso pueda producirse indefensión.

En segundo lugar, procede citar la **Sentencia de 8 de octubre de 2024, núm. 1568/2024 que resuelve el Recurso de Casación núm. 1920/2021**, interpuesto por la Agencia Española de Protección de la Salud en el Deporte, frente a la Sentencia de la Audiencia Nacional de 24 de noviembre de 2020, que desestima las pretensiones de la recurrente y confirma la declaración de infracción que hace la resolución de la Agencia. El del recurso es desfavorable al recurrente fijando la siguiente doctrina casacional:

El artículo 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con lo dispuesto en el artículo 4.15 y el considerando 35 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), debe interpretarse en el sentido de que los datos de carácter personal referidos a información sobre el estado de salud física o mental de los deportistas, relacionados con la aplicación de las técnicas del control de dopaje, (como los concernientes a la detección de la presencia de sustancias dopantes o de resultado de pruebas analíticas antidopaje), tienen el carácter tipológico o categorial de datos relativos a la salud, a los efectos de que el tratamiento, cesión o comunicación de dichos datos goce de la protección reforzada que contempla la normativa estatal y la legislación de la Unión Europea sobre protección de datos personales aplicable.

En tercer lugar, procede citar la **Sentencia de 4 de marzo de 2024, núm. 374/2024 que resuelve el Recurso de Casación núm. 7418/2022**, interpuesto por un particular contra la sentencia de 17 de junio de 2022 la Audiencia Nacional que confirma la desestimación que hace la Agencia frente a la solicitud del derecho de supresión que hace el recurrente en relación a 18 enlaces web que muestran los datos personales de su padre fallecido como secretario judicial del Juzgado Militar de Prensa que condenó al poeta Miguel Hernández.

El recurrente sostiene que existen inexactitudes en las publicaciones objeto de análisis, que el tribunal considera irrelevantes a los efectos de la ponderación realizada de los derechos e intereses en conflicto.

Entiende la Sala que *la sentencia impugnada acierta al considerar como elementos relevantes, obstativos del derecho de supresión ejercitado, que las informaciones revistiesen un interés público incuestionable al versar sobre la intervención del padre del recurrente, como secretario judicial del Juzgado Especial de Prensa que instruyó la causa penal contra el poeta Miguel Hernández; que la información aparecida formara parte de una investigación histórica y científica, contenida en publicaciones de la Universidad; y que el transcurso del tiempo no hubiese hecho decaer el interés que suscita todo lo que rodea a la muerte del famoso poeta.*

Así mismo, resulta acertado que, al tiempo de valorar las inexactitudes aducidas por los recurrentes, se tuviese en consideración que se trababan de errores circunstanciales que no afectaban a la esencia de lo informado ni a la exactitud del conjunto de la información tratada A tal efecto, la sentencia razona «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 Sr. B. 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(documento 1 de la contestación) y en dichas publicaciones no se le atribuye un papel distinto del de secretario del órgano judicial.

Y añade «El hecho de que el Sr. B., 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».

Consideramos, por tanto, que la sentencia de la Audiencia Nacional aplicó correctamente tanto la legislación como la jurisprudencia existente cuando frente al ejercicio del derecho de supresión ejercido por los familiares del difunto se ponderaron otros derechos e intereses concurrentes y se valoró, acertadamente, el alcance de la inexactitud en relación con el conjunto y contexto de la información tratada.

Tras el análisis establece la siguiente doctrina: *El derecho de supresión (derecho al olvido) de los datos de una persona fallecida está reconocido en nuestro ordenamiento. Pero, la singularidad que implica que el derecho de supresión se ejercite respecto de datos personales correspondientes a una persona fallecida no suprime la necesidad de ponderar la protección de datos del difunto con otros derechos y libertades en conflicto a la luz de nuestras normas y de la jurisprudencia existente.*

Alegada la inexactitud parcial de una información que afecta a una persona fallecida, y que aparece incorporada a una investigación histórica y científica, la exigencia de exactitud de lo afirmado se aminora y debe ponderarse también la trascendencia de la inexactitud en el conjunto de la información aparecida.

Finalmente, destaca la **Sentencia de 8 de octubre de 2024 núm. 1569/2024 recaída en el Recurso de Casación 3120/2023**, interpuesta por una compañía de telefonía y que aborda el tratamiento de datos personales derivado de la ya citada estafa de duplicados de tarjetas SIM en relación con la vulneración del principio de confidencialidad, por cuanto se debatía sobre el encaje de estas conductas en la vulneración del citado principio.

La Sala establece la siguiente doctrina: *El artículo 5.1 f) del RGPD, resulta aplicable a aquellas conductas consistentes en que el responsable o el encargado del tratamiento de datos o sus empleados, faciliten el acceso a los datos personales contenidos en la tarjeta SIM a terceros, mediante la generación de duplicados obtenidos de forma fraudulenta, por no adoptar las medidas de seguridad adecuadas para evitar tratamiento no autorizados o ilícitos, al poner en riesgo la integridad y la confidencialidad de los datos.*

Por último, en cuanto a la jurisprudencia del Tribunal de Justicia de la Unión Europea dictadas durante el ejercicio 2024, procede destacar las siguientes.

Sentencia de 4 de octubre 2024 Asunto C-446/2021 que aborda los principios de limitación de la finalidad y minimización, así como el análisis sobre las causas que levantan la prohibición de tratamiento de categorías especiales de datos.

El responsable del tratamiento es la empresa propietaria de una red social que, mediante distintos sistemas, herramientas y servicios, recaba datos personales de los usuarios y los almacena para ofrecer publicidad personalizada. Por otro lado, los hechos también se refieren al tratamiento de categorías especiales de datos recabados fuera de la red social que el recurrente ha hecho públicos y que luego la red social utiliza.

La Sentencia, tras analizar las disposiciones aplicables concluye que *el principio de «minimización de datos» se opone a que todos los datos personales que un responsable del tratamiento, como el operador de una plataforma de red social en línea, haya obtenido del interesado o de terceros y que hayan sido recogidos tanto en dicha plataforma como fuera de esta se agreguen, se analicen y se traten a efectos de proponer publicidad específica, sin limitación temporal y sin distinción en función de la naturaleza de esos datos.*

Y, en segundo lugar, que el hecho de que una persona se haya manifestado sobre su orientación sexual en una mesa redonda abierta al público no autoriza al operador de una plataforma de red social en línea a tratar otros datos relativos a la orientación sexual de esa persona obtenidos, en su caso, fuera de dicha plataforma a partir de aplicaciones y de sitios de Internet de terceros asociados, con el fin de agregar y de analizar tales datos para proponerle publicidad personalizada.

Sentencia de 11 de julio de 2024, Asunto C-461/22, que trata aborda la consideración de un curador respecto de las gestiones que realizó respecto de la persona sometida a curatela y los derechos que a esta le asisten. La controversia surge cuando la persona sometida a curatela ejerce el derecho de acceso previsto en el artículo 15 del RGPD en relación con la actuación de su antiguo curador.

La Sentencia examina conjuntamente si el artículo 4.7, del RGPD debe interpretarse en el sentido de que un antiguo curador que ha ejercido sus funciones a título profesional respecto de una persona sujeta a su curatela debe calificarse de «responsable del tratamiento», en el sentido de dicha disposición, de los datos personales en su posesión relativos a esa persona y de que dicho tratamiento debe respetar todas las disposiciones del mencionado RGPD, en particular su artículo 15. La conclusión es afirmativa en ambos aspectos.

Sentencia de 7 de marzo de 2024, Asunto C-604/22, aborda entre otras cuestiones qué se considera dato de carácter personal, y realiza una interpretación extensiva del concepto, al concluir que una cadena compuesta por una combinación de letras y caracteres, que contiene las preferencias de un usuario de Internet o de una aplicación relativas al consentimiento de dicho usuario en el tratamiento de datos personales que le conciernen por proveedores de sitios de Internet o de aplicaciones, así como por intermediarios de tales datos y por plataformas publicitarias, constituye un dato personal, en el sentido del artículo 4.1 del RGPD, en la medida en que, cuando puede asociarse, por medios razonables, a un identificador, como en particular la dirección IP del dispositivo de dicho usuario, permite identificar al interesado.

En tales circunstancias, el hecho de que, sin una contribución externa, una organización sectorial que posee esta cadena no pueda acceder a los

datos tratados por sus miembros en el marco de las normas que ella ha establecido ni combinar dicha cadena con otros elementos no impide que la mencionada cadena constituya un dato personal.

Sentencia de 7 de marzo de 2024, Asunto C-740/22 que analiza la comunicación oral de información sobre condenas penales y su consideración como tratamiento de datos personales en el sentido del RGPD.

Los hechos son que la recurrente, una entidad mercantil oralmente al Tribunal Primera Instancia de la Región de Savonia del Sur, Finlandia, información sobre posibles condenas penales pendientes o ya cumplidas relativa a una persona física que participaba en un concurso organizado por dicha sociedad, con el fin de determinar los antecedentes judiciales de esta persona. Frente a ello el tribunal desestimo la solicitud.

La Sentencia resuelve que la comunicación oral de información sobre posibles condenas penales pendientes o ya cumplidas relativa a una persona física constituye un tratamiento de datos personales, en el sentido del artículo 4.2 del RGPD, que está comprendido en el ámbito de aplicación material de este cuando dicha información está contenida o destinada a ser incluida en un fichero.

Sentencia de 11 de julio de 2024, Asunto C-757/22 que considera que una asociación de consumidores está legitimada para interponer una acción contra la vulneración de la normativa de protección de datos, aunque no disponga de un mandato a tal efecto.

Para que una entidad tenga legitimación activa para interponer una acción, basta con que el tratamiento de datos en cuestión pueda afectar a los derechos previstos en el RGPD, y no es necesario demostrar que se ha producido un daño real al interesado.

La Sala considera que: *se cumple el requisito según el cual, para ejercitar una acción de representación con arreglo al artículo 80.2 del RGPD, una entidad debe alegar que considera que los derechos del interesado conferidos por el RGPD han sido vulnerados «como consecuencia de un tratamiento», cuando dicha entidad alega que la vulneración de los derechos de esa persona se produce con ocasión de un tratamiento de datos personales y se deriva del incumplimiento de los artículos 12.1 y 13.1 letras c) y e), RGPD, en concreto, de comunicar al interesado afectado por ese tratamiento de datos, de forma concisa, transparente, inteligible y fácilmente accesible, con un lenguaje claro y sencillo, la información relativa a los fines de ese tratamiento de datos y a los destinatarios de los mismos, a más tardar en el momento de su recogida*.

Sentencia de 14 de marzo de 2024, Asunto C-46/23, que considera que la autoridad de control de un Estado miembro está facultada, en ejercicio de sus poderes correctivos, para ordenar al responsable o al encargado del tratamiento que suprima datos personales que hayan sido tratados ilícitamente, aun cuando el interesado no haya presentado ninguna solicitud a tal efecto para ejercer sus derechos en virtud del artículo 17.1 del RGPD.

Finalmente citar las **Sentencias de 4 de octubre de 2024, Asunto C-200/23** que considera la firma manuscrita como dato personal y la relativa al **Asunto C-21/13** que considera dentro de las categorías especiales de datos, en concreto dato relativo a la salud, el tratamiento consistente en introducir por un farmacéutico en una plataforma online los datos de nombre y apellidos y dirección de envío para solicitar un medicamento, aun cuando la venta de este no esté sujeta a receta médica.

2.7 Tecnológicos

2.7.1 Gestión de notificaciones de brechas de datos personales

El artículo 33 del RGPD establece la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas. Esta obligación forma parte de la **responsabilidad proactiva** del responsable del tratamiento de datos.

La notificación a la autoridad de control debe realizarse **sin dilación indebida y a más tardar en 72 horas** desde que la organización tiene constancia de la brecha. La falta de cumplimiento de esta obligación está tipificada como infracción. La **Agencia Española de Protección de Datos (AEPD)** es la autoridad de control en España, aunque las Comunidades Autónomas de Andalucía, Cataluña y País Vasco tienen sus propias autoridades de control para entidades del sector público bajo su competencia.

La AEPD facilita una herramienta llamada **ASESORA BRECHA** para ayudar a los responsables a valorar el riesgo y decidir si notificar una brecha de datos. Las notificaciones a la AEPD deben realizarse de **forma electrónica** a través del formulario de notificación de brechas de datos personales disponible en la Sede Electrónica de la AEPD. La AEPD también ofrece una **guía** para la notificación de brechas de datos personales, que tiene como objetivo ayudar a los responsables a cumplir con sus obligaciones de notificación y comunicación a los afectados. El responsable del tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo. Además, cuando el riesgo sea alto, el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD. Si el responsable considera que no existen riesgos para los derechos y libertades de las personas físicas, tiene la obligación de documentar cualquier violación de la seguridad de los datos personales. La notificación de una brecha de datos personales a la AEPD y la comunicación de una brecha de datos personales a los interesados, son evidencias de la diligencia de la organización. No obstante, **el incumplimiento de la obligación de notificar** a la autoridad de control y, cuando proceda, de **comunicar a los interesados**.

> La obligación que establece el artículo 33 del RGPD, se ha materializado a lo largo del año 2024 en un total de **2.933 notificaciones de brechas de datos personales** lo que viene a suponer un incremento que supera el 46% con relación a las notificaciones de brechas que los responsables notificaron a la AEPD. De las notificaciones de brecha recibidas aproximadamente el **16% corresponde al sector público y el 84% corresponden al sector privado**.

En general, las brechas que afectan a un número más elevado de personas son las relacionadas con ciberincidentes de tipo ransomware e intrusiones en sistemas de información que resultan en exfiltración de grandes volúmenes de datos personales. Este tipo de brechas afecta tanto a entidades públicas como privadas.

Como consecuencia de las notificaciones recibidas se han emitido un total de **13 resoluciones para obligar a los responsables a comunicar las brechas a los interesados** y se ha dado traslado a la Subdirección General de Inspección de Datos un total de 15 notificaciones al objeto de que se realizara un segundo análisis más exhaustivo.

Como resultado de la información aportada en las notificaciones recibidas, el número total de interesados que han podido ser objeto de una comunicación de brecha de datos personales en los términos que establece el artículo 34 del RGPD aumenta en 2024, superando la cifra de **100 millones de interesados que podrían verse afectados** en mayor o menor grado por una brecha.

La AEPD colabora estrechamente con las autoridades autonómicas de protección de datos en la gestión de las notificaciones de brechas de datos personales.

Esta colaboración se materializa en:

- **Reuniones Monográficas:** Se han celebrado dos reuniones específicas en 2024, una en marzo en la sede de la Agencia Vasca de Protección de Datos (AVPD) en Vitoria y otra en noviembre en la sede de la AEPD en Madrid, donde las autoridades compartieron procedimientos y experiencias para armonizar sus actuaciones.

- **Traslado de Notificaciones:** La AEPD ha transferido 7 notificaciones de brechas a las autoridades autonómicas al determinar que el tratamiento afectado por la brecha se encontraba dentro del ámbito de su competencia.

Este esfuerzo conjunto busca **garantizar una aplicación coherente del Reglamento General de Protección de Datos (RGPD)** y una cooperación efectiva entre las distintas autoridades de control. La colaboración incluye la asistencia mutua y el intercambio de información útil para aplicar el reglamento de manera uniforme.

2.7.2 Consultas previas

El artículo 36 del RGPD establece la obligación de **consultar a la autoridad de control** sobre la procedencia de una actividad de tratamiento, siempre antes de iniciarla, cuando una evaluación de impacto relativa a la protección de datos (EIPD) muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, dicho tratamiento entrañaría un **alto riesgo** para los derechos y libertades de las personas físicas.

La consulta previa **no es una acción aislada**, sino que debe integrarse en la estrategia de gestión del riesgo para los derechos y libertades a la que obliga el RGPD. No se trata de una simple remisión de la EIPD a la autoridad de control, sino que implica una colaboración activa con la autoridad, el seguimiento del proceso y facilitar toda la información adicional que precise durante el proceso de evaluación.

Según la información proporcionada, a lo largo de 2024 se recibieron un total de **32 consultas previas** basadas en el artículo 36 del RGPD. De estas, **22 no cumplían** los requisitos de consulta previa exigidos en los artículos 35 y 36 del RGPD. Además, **10 consultas previas** planteaban dudas sobre el cumplimiento de las obligaciones generales del RGPD, que deberían haber sido resueltas con el asesoramiento del Delegado de Protección de Datos (DPD).

Las consultas previas recibidas dieron lugar a **17 informes de respuesta**, donde se destaca una interpretación errónea sobre la relación entre cumplimiento y gestión del riesgo, ya que se entienden como idénticos. También se identifica una **interpretación errónea sobre la finalidad de la consulta previa**. En lugar de entenderla como un asesoramiento de la autoridad de control sobre los riesgos no mitigados adecuadamente, se busca una validación previa de la EIPD por parte de la autoridad.

La AEPD ofrece orientaciones y modelos para documentar el resultado de la EIPD y facilitar la labor del responsable al realizar una consulta previa. Sin embargo, estas herramientas no deben confundirse con el concepto de gestión del riesgo, que no es un documento sino un proceso continuo.

En cuanto a la función consultiva de la AEPD, esta se enfoca en:

- **Actividad normativa:** Asesoramiento sobre la normativa de protección de datos.

- **Información a ciudadanos:** Atención a consultas sobre sus derechos en materia de protección de datos.

- **Consultas de los DPD:** Respuesta a consultas de los DPD bajo ciertos requisitos.

- **Consultas previas:** Atención a consultas previas en base al artículo 36 del RGPD.

Es importante tener en cuenta que **la AEPD no desarrolla funciones consultivas individualizadas** destinadas a responsables y encargados del tratamiento. La responsabilidad proactiva recae en los responsables del tratamiento, quienes deben poder demostrar el cumplimiento de la normativa, con el apoyo de sus DPD, abogados o consultores.

La AEPD puede ejercer sus **poderes de investigación y supervisión** ante la información remitida por el responsable en una consulta previa. Esto puede incluir la solicitud de información adicional, la realización de auditorías y la imposición de sanciones en caso de incumplimiento.

2.7.3 Acciones realizadas desde la DIT y recursos de utilidad publicados

En línea con la implicación de la DIT en relación con la protección del menor, en especial, con el **acceso de menores a contenidos no adecuados** para su edad se han realizado acciones de asesoramiento nacional e internacional que han supuesto más de 80 reuniones en las que se ha venido a compartir la experiencia de la DIT con entidades públicas y privadas que han mostrado su interés en la solución planteada para la verificación de edad en internet desde la AEPD, dando lugar a las siguientes publicaciones:

- **Informe sobre la influencia de los patrones adictivos en Internet, y en especial sobre los menores de edad**
- **Nota Técnica: Internet seguro por defecto para la infancia y el papel de la verificación de edad**
- **Responsabilidades y obligaciones en la utilización de dispositivos móviles en la enseñanza infantil, primaria y secundaria**
- **Proteger a nuestros hijos e hijas en el mundo digital: El internet del hogar (router Wifi)**
- **Annual Privacy Forum 2.024: Implications of Age Assurance on Privacy and Data Protection: A Systematic Threat Model**
- **Responsabilidades y obligaciones en la utilización de dispositivos móviles en la enseñanza infantil, primaria y secundaria**
- **Nota Técnica: Patrones adictivos y el derecho a la integridad de la persona**

Con relación a la gestión del riesgo ha sido publicada una introducción a la **metodología de modelado de amenazas para la privacidad y la protección de datos LIINE4DU 1.O** que supone la continuidad de la ya larga trayectoria de la AEPD a los trabajos realizados en años anteriores con relación a la gestión del riesgo y la evaluación de impacto en protección de datos, línea de trabajo que complementa las acciones de gestión de riesgos y que pretende ayudar a comprender, de manera sistemática, el análisis de las consecuencias no deseadas que pueden resultar de un tratamiento de datos personales.

En esta línea de gestión del riesgo se ha prestado especial atención a la evolución a las herramientas existentes, realizando mejoras en la herramienta **GESTIONA-RGPD** con nuevas funcionalidades que ayudan a la gestión del RAT y la generación del inventario de actividades de tratamiento a la vez que se ha dotado a la herramienta de un **manual de ayuda**.

Esta evolución de las herramientas ya publicadas, a lo largo de 2024, ha supuesto la realización de una actualización tecnológica de los asistentes **FACILITA-RGPD**, **FACILITA-EMPRENDE**, **ASESORA-BRECHA** y **COMUNICA-BRECHA** y, por otra parte, también se ha colaborado con la Subdirección General de Promoción y Autorizaciones en el desarrollo del portal de violencia de género, actualizaciones que siguen en evolución durante el año 2025.

Especialmente relevante es el esfuerzo de prospección realizado desde la DIT para dar continuidad al trabajo necesario para cumplimiento del RGPD en el ámbito de la tecnología **blockchain**, manteniendo la participación en los grupos del EDPB con un total que supera las veinte participaciones de los expertos de la DIT en grupos de expertos tanto nacionales como internacionales y cuyo resultado se encuentra reflejado en los siguientes documentos:

- **Nota técnica: Prueba de concepto Blockchain y el derecho de supresión** donde se analiza las implicaciones de esta tecnología de almacenamiento e intercambio distribuido de información con relación a la normativa de protección de datos.

- **Anexo Descripción técnica Prueba de Concepto Blockchain y el derecho de supresión**

- **Video: Prueba de concepto Blockchain y el derecho de supresión**

Desde la DIT se han desarrollado y publicado guías, artículos y notas técnicas de diversa índole como los que se indican a continuación:

- **Interés vital y protección de datos:** analiza cómo el supuesto de interés vital se encuadra en el marco de la protección de datos personales. Expone las circunstancias en las que se permite el tratamiento de datos sin consentimiento, cuando es indispensable para salvaguardar intereses fundamentales como la vida o la integridad física de una persona. Asimismo, discute el equilibrio necesario entre la aplicación de esta excepción y el respeto a los derechos fundamentales, ofreciendo criterios y recomendaciones para su correcta interpretación y aplicación en situaciones de urgencia.

- **Brechas de datos personales: seguridad enfocada a los tratamientos:** examina la importancia de establecer medidas de seguridad robustas en el tratamiento de datos personales para prevenir, detectar y responder a incidentes de brechas de seguridad. Se analizan las obligaciones legales establecidas por el RGPD en cuanto a la notificación y gestión de dichas brechas, y se destacan buenas prácticas y medidas técnicas y organizativas que aseguren la integridad, confidencialidad y disponibilidad de la información. Además, se enfatiza la necesidad de una cultura de seguridad proactiva y de una respuesta coordinada y efectiva ante incidentes,

- **Identidad como derecho:** El documento analiza las implicaciones de tratar la identidad como un servicio en lugar de como un derecho fundamental y cómo la evolución hacia la identidad como servicio afecta al control que tienen las personas sobre sus datos personales. La mercantilización de la identidad puede afectar a los derechos y libertades de las personas, a la inclusión social y a la igualdad, e implica diferentes consideraciones éticas. ¿Cómo pueden los gobiernos equilibrar la prestación de servicios de identidad con la protección de los derechos fundamentales y la autonomía de los ciudadanos.

Con relación a las cookies y a las herramientas de medición de audiencia basadas en esta tecnología de seguimiento fue publicada la **Guía para de Uso de cookies para herramientas de medición de audiencia**. Este documento tiene como propósito ofrecer un conjunto de orientaciones y recomendaciones destinadas a los responsables de sitios web y aplicaciones que emplean cookies para el análisis y seguimiento del comportamiento de los usuarios, a fin de mejorar la medición de la audiencia y la eficacia de los servicios digitales y se configura como un recurso imprescindible para aquellas organizaciones que buscan equilibrar la necesidad de obtener información analítica sobre el comportamiento de los usuarios con el imperativo de proteger sus derechos fundamentales en materia de privacidad. Al proporcionar orientaciones detalladas sobre la obtención del consentimiento, la minimización de riesgos y la implementación de medidas de seguridad. La guía contribuye a fomentar una cultura de transparencia y responsabilidad en el tratamiento de datos personales en el entorno digital. De este modo, se promueve un uso ético y conforme a la normativa de las tecnologías de seguimiento, facilitando una medición de audiencia que respete plenamente los estándares de protección de datos.

2.7.4 Elaboración de recursos y documentación en colaboración con otras autoridades

Uno de los ejes estructurales de la División de Innovación Tecnológica (DIT) es la estrecha colaboración con las autoridades, lo que se ha traducido en una coordinación constante y eficaz con las administraciones autonómicas. Durante el año 2024, esta colaboración ha tomado un protagonismo especial al materializarse en el desarrollo de una guía práctica orientada a los responsables de actividades de tratamiento que implican el rastreo de dispositivos a través de las señales Wi-Fi que estos emiten. El rastreo de dispositivos mediante la captura de señales Wi-Fi representa una tecnología con un potencial significativo para optimizar procesos y mejorar

servicios en distintos sectores, desde la gestión de espacios públicos hasta la personalización de experiencias comerciales. No obstante, su implementación conlleva riesgos sustanciales para la privacidad, dado que muchas veces las personas afectadas no son plenamente conscientes de que sus dispositivos emiten señales que pueden ser interceptadas y analizadas. Esto se agrava cuando la actividad se lleva a cabo sin contar con una base legal adecuada que autorice y regule dicho tratamiento de datos.

Conscientes de estas implicaciones, la DIT, en colaboración con las autoridades autonómicas, ha desarrollado la «Guía de Tecnologías de Seguimiento WI-FI: Orientaciones para responsables del tratamiento».

Este documento constituye una herramienta clave que cumple varias funciones:

1. **Orientación Técnica y Normativa:** proporciona un marco de referencia tanto para los responsables del tratamiento como para los técnicos que implementan estas tecnologías. Se detallan los procedimientos y protocolos recomendados para asegurar que el rastreo de dispositivos se realice en conformidad con el Reglamento General de Protección de Datos (RGPD) y la legislación nacional. Asimismo, se especifican los criterios técnicos que deben cumplirse para minimizar el riesgo de identificación no autorizada y garantizar la anonimización de los datos en la medida de lo posible.

2. **Análisis de Riesgos y Evaluación de Impacto:** realiza un análisis exhaustivo de las posibles implicaciones de la tecnología de seguimiento Wi-Fi. Este análisis identifica los principales riesgos asociados al tratamiento de datos derivados de la captura de señales, como la invasión a la privacidad, la posibilidad de vigilancia no consentida y el riesgo de explotación comercial de datos sensibles. La guía enfatiza la necesidad de realizar evaluaciones de impacto en la protección de datos (DPIA, por sus siglas en inglés) que permitan a los responsables valorar de forma proactiva las vulnerabilidades y adoptar medidas correctivas y preventivas.

3. **Recomendaciones y Buenas Prácticas:** propone recomendaciones prácticas que pueden servir de salvaguarda para proteger los derechos y libertades de las personas físicas. Entre estas recomendaciones se incluyen:

   - La adopción de técnicas de minimización de datos, asegurando que únicamente se recoja la información estrictamente necesaria para los fines establecidos.
   - La implementación de medidas de seguridad avanzadas para evitar accesos no autorizados o el uso indebido de la información recabada.
   - La garantía de transparencia mediante la notificación a los ciudadanos sobre la existencia y funcionamiento de estos sistemas de rastreo, así como la obtención del consentimiento explícito cuando sea procedente.
   - La revisión y actualización periódica de los protocolos y sistemas, de forma que se adapten a las evoluciones tecnológicas y a las modificaciones en el marco normativo.

4. **Implicaciones Legales y de Responsabilidad:** aborda el aspecto jurídico, subrayando la importancia de contar con una base legal sólida para el tratamiento de datos personales derivados de la captura de señales Wi-Fi. Se analiza la situación actual de la normativa y se orienta a los responsables sobre cómo proceder en aquellos casos en que la actividad pueda estar en conflicto con los principios del RGPD. Esto incluye la evaluación de los fundamentos legales que podrían justificar el tratamiento y la documentación de los procedimientos para demostrar el cumplimiento normativo.

5. **Fomento de la Cultura de Protección de Datos:** Finalmente, la iniciativa forma parte de un esfuerzo más amplio para promover una cultura de protección de datos en el entorno tecnológico. La DIT, mediante esta guía, no solo pretende ofrecer una solución práctica a un problema emergente, sino también sensibilizar a los actores involucrados sobre la importancia de respetar los derechos fundamentales en un entorno cada vez más digitalizado.

En resumen, la Guía de Tecnologías de Seguimiento WI-FI representa una respuesta integral a los desafíos que plantean las nuevas tecnologías de rastreo. Al ofrecer orientaciones detalladas, análisis de riesgos y recomendaciones prácticas, la DIT y las autoridades autonómicas buscan asegurar que el uso de estas tecnologías se realice de forma responsable, transparente y respetuosa con la privacidad de los ciudadanos, consolidando así una base sólida para el tratamiento de datos en el entorno digital.

Como resultado y continuación de la **Conferencia Internacional AEPD-ENISA sobre Espacios de Datos** europeos celebrada octubre de 2023, ha sido publicado el **Informe de conclusiones del evento de AEPD-ENISA sobre espacios de datos** en el que se pone de manifiesto que los espacios de datos se constituirán como un hub común en el que convergerán todas las tecnologías actuales y futuras y sobre el que será posible la obtención de nuevos beneficios para nuestra sociedad, siempre que dichas infraestructuras tecnológicas se constituyan como un entorno de confianza para los legítimos titulares de los datos. Dentro del ámbito de la colaboración con ENISA ha sido también desarrollado un documento sobre **Ingeniería de protección de datos personales en los espacios de datos de la UE**, documento que pretende proporcionar garantías de diseño en el desarrollo de los espacios comunes europeos de datos con el objetivo de impulsar el crecimiento y la innovación europeos aplicando la ingeniería de protección de datos no como una mera estructura para el cumplimiento formal de las previsiones de las normativas de protección de datos personales sino como una forma eficiente y dinámica para la protección de los derechos y libertades de las personas físicas dando respuesta a las consideraciones relativas a las medidas técnicas y organizativas adecuadas a cada caso concreto de espacio de datos.

Dentro del marco de la colaboración con el EDPS (Oficial Europeo de Protección de Datos), se ha publicado el documento "TechDispatch: Neurodatos", que se erige como un hito en el análisis de las implicaciones derivadas del uso de la neurotecnología en el tratamiento de datos neurológicos.

Este documento examina de forma exhaustiva los desafíos y riesgos que plantea la incorporación de neurodatos en entornos tecnológicos, con especial atención a los aspectos relacionados con la protección de datos y los derechos fundamentales.

Entre los **puntos clave** que aborda este documento se encuentran:

1. **Sensibilidad de la Información Neurológica:** El documento destaca que los neurodatos, al estar directamente vinculados a la actividad cerebral, tienen una sensibilidad y carácter íntimo que supera, en muchos casos, al de otros tipos de datos personales. Esto implica que cualquier tratamiento de esta información requiere medidas de seguridad y protección excepcionalmente rigurosas para evitar vulneraciones a la privacidad y a la integridad personal.

2. **Implicaciones para la Privacidad y la Autonomía Individual:** La neurotecnología no solo permite la recogida de datos sobre la actividad cerebral, sino que, en algunos casos, también posibilita la intervención o manipulación de funciones neurológicas. Estas capacidades abren un debate ético y jurídico en torno a la preservación del libre albedrío, la identidad personal y la privacidad mental, aspectos que el documento analiza detalladamente en el contexto de los marcos normativos actuales.

3. **Riesgos y Desafíos Regulatorios:** TechDispatch: Neurodatos examina los riesgos inherentes al tratamiento de neurodatos, tales como el potencial uso indebido de la información para fines de vigilancia o manipulación, y la posible falta de bases legales adecuadas que legitimen el procesamiento de estos datos. El documento subraya la necesidad de establecer normativas específicas o adaptar las existentes (como el RGPD) para cubrir las particularidades que presenta el tratamiento de neurodatos, garantizando siempre un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales.

4. **Recomendaciones para una Gestión Responsable:** Con el objetivo de orientar tanto a responsables de tratamiento como a legisladores y desarrolladores, el documento ofrece una serie de recomendaciones prácticas y estratégicas. Entre ellas se incluyen:

   - La adopción de medidas de minimización y anonimización de datos que reduzcan al máximo el riesgo de identificación de personas.
   - La implementación de evaluaciones de impacto específicas para el tratamiento de neurodatos, permitiendo identificar y mitigar riesgos de forma proactiva.
   - La necesidad de una mayor transparencia y de la obtención de un consentimiento informado claro por parte de los usuarios, que contemple las particularidades del procesamiento de datos neurológicos.
   - La promoción de un marco ético que integre consideraciones sobre la autonomía personal y la integridad mental, aspectos esenciales en el contexto de la neurotecnología.

5. **Contribución al Debate Internacional:** Además de su relevancia a nivel europeo, el TechDispatch: Neurodatos se posiciona como un documento de referencia a nivel internacional. En él se plantean fundamentos y argumentos que pueden servir de base para futuras normativas y directrices globales, orientadas a regular el uso de la neurotecnología de forma ética y responsable, y a garantizar que el progreso en este campo se realice respetando los derechos humanos.

Desde el Comité Europeo de Protección de Datos (EDPB) la DIT ha participado en el desarrollado del **Dictamen 11/2024 sobre tratamientos biométricos en aeropuertos**, un documento técnico y normativo que aborda de forma exhaustiva las particularidades y desafíos asociados al tratamiento de datos biométricos en el entorno aeroportuario. Este dictamen surge de la necesidad de conciliar el uso creciente de tecnologías biométricas para fines de seguridad y control en los aeropuertos con el imperativo de proteger los derechos fundamentales de los ciudadanos, en especial el derecho a la privacidad y la protección de datos personales.

Por otra parte, se participa activamente en el EDPB en el desarrollo de la opinión sobre "**Interplay RGPD-AIA**" y también se continúa colaborando en el desarrollo de la actualización del **Dictamen sobre anonimización** ya mencionado.

Como continuación de las acciones realizadas en 2023 en inteligencia artificial y decisiones automatizadas se han publicado los artículos siguientes:

- **Datos e información en Inteligencia:** aborda la relevancia y los desafíos asociados al uso de datos en el ámbito de la inteligencia artificial. Se analizan aspectos como la calidad y el tratamiento de la información, la necesidad de una adecuada gobernanza de datos y el cumplimiento de normativas (por ejemplo, el RGPD). Además, se exploran las implicaciones éticas y los posibles sesgos derivados de la utilización masiva de datos en sistemas de IA, proponiendo orientaciones para garantizar la transparencia, la integridad y la seguridad en el procesamiento de la información.

- **Evaluación de la intervención humana en las decisiones automatizadas:** En el que se analiza la necesidad de realizar una evaluación del grado de participación humana, lo que implica evaluar tanto el sistema utilizado como el tratamiento y su contexto. Para ello, se recomienda valorar la participación de una persona en el proceso de decisión examinando diferentes aspectos, como su autoridad, competencia, capacidad, diligencia o independencia.

La DIT continúa colaborando con la **SEDIA en el Grupo del Dato** mediante una ponencia sobre anonimización a fin de impulsar este requisito que exige el artículo 32 del RGPD como garantía de privacidad.

2.7.5 Proyección internacional en responsabilidad proactiva y ámbito tecnológico

En el ámbito de la proyección internacional, la DIT colabora estrechamente con la División de Relaciones Internacionales y las actividades que se han desarrollado pueden agruparse de la siguiente forma:

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS:

- Participación en el Subgrupo de Tecnología
- Finalización del proyecto EDPB/Eticas sobre IA
- Ponentes en la guía de Blockchain
- Ponentes en la declaración de verificación de edad.
- Co-ponentes en la “Guía de anonimización”
- Co-ponentes en la "Guía de seudonimización"
- Co-ponentes en el drafting team del interplay AIA-GDPR
- Participación en el Mobile Apps Expert Exchange
- Questions on SMEs & Días
- Co-ponentes en el Dictamen 11/2024 sobre el uso del reconocimiento facial para agilizar el flujo de pasajeros en aeropuertos (compatibilidad con los artículos 5, apartado 1, letras e) y f) y 25 y 32, antes mencionado

ENISA:

- Publicación ENISA Engineering Personal Data Sharing (coponentes) y traducción al castellano de la misma.
- Participación como observadores en el ENISA's Ad-Hoc Working group en Ingeniería de la Privacidad, en el Advisory Group y en comité de revisión del Anual Privacy Forum.
- Realización de informe conjunto sobre las conclusiones del evento de AEPD-ENISA sobre espacios de datos realizado en 2023.

RELACIÓN CON OTRAS AUTORIDADES Y ORGANISMOS PÚBLICOS INTERNACIONALES:

- Colaboración con el EDPS en la elaboración de un TechDispatch conjunto sobre neurodatos y la realización de un podcast conjunto.
- Colaboración con la CNIL en herramientas sobre brechas de datos
- Participación en la TaskForce ChatGPT
- Participación en el Working group CA@AI Grupo de Autoridades Europeas Competentes
- Observadores del European Blockchain Regulatory Sandbox
- Participación en la declaración sobre Data Scrapping impulsada en la GPA
- Colaboración con la autoridad de protección de datos de Singapur en relación a datos sintéticos.
- Participación con el grupo de Berlín con relación a neurodatos.
- Protocolo de colaboración con la Universidad de las Naciones Unidas en el campo de Blockchain
- Task Force y prueba piloto de la Comisión Europea para la verificación de edad
- European Board for Digital Services, working group 6 para la elaboración de las Guidelines sobre el artículo 28 de la DSA

ORGANISMOS DE ESTANDARIZACIÓN

- ISO: Co-editores estándar ISO 27574 “Privacy in brain-computer interface (BCI) applications”
- ISO verificación de edad ISO/IEC JTC 1/SC 27/ WG 5
- Vocal UNE CTN-71 Tecnologías Habilitadores Digitales
- Vocal UNE CTN-320 Seguridad y protección de datos

LÍDERES DEL COMPONENTE DE PROTECCIÓN DE DATOS DEL TWINNING DE LA UNIÓN EUROPEA PARA LA DIGITALIZACIÓN DE UCRANIA-EU4DIGITALUA:

- Organización de una conferencia Internacional en Varsovia AEPD-Autoridad Ucraniana-Autoridad Polaca
- Firma de un MoU de colaboración con la Autoridad Ucraniana
- Realización de dos acciones de Internship con un total de 7 miembros de la Autoridad Ucraniana
- Desarrollo de un workshop online sobre las herramientas de la AEPD.
- Desarrollo de tres actividades relativas a protección de datos en AA.PP., Retirada de Contenidos, Inteligencia Artificial.
- Organización de un workshop sobre la protección de menores en Internet.
- Realización de un ciclo de seis seminarios sobre protección de datos y nuevas tecnologías para el Ministerio de Transformación Digital Ucraniano.

2.7.6 Publicaciones, formación y acciones de difusión

Las acciones de difusión realizadas desde la DIT vienen a dar respuesta a los nuevos planteamientos que los desarrollos tecnológicos suponen con relación a la privacidad y la protección de los derechos y libertades de las personas físicas. En particular cuando estos desarrollos tecnológicos son novedosos, o bien, cuando se muestran errores de concepto en las consultas planteadas a la AEPD o en los foros en los que participan miembros de esta División.

En colaboración con el Gabinete de Prensa se ha elaborado una **artículo en el blog** para divulgar las diferentes herramientas que la AEPD ofrece a responsables y encargados de tratamiento.

Con relación a las personas mayores y la posible discriminación que podrían sufrir como resultado de una **digitalización sin alternativas adecuadas**, se ha publicado una nota de blog en la que la AEPD advierte de las posibles consecuencias que un aumento en los fenómenos de exclusión de las personas mayores en los servicios digitales puede tener en función de la edad de una persona adulta, viniendo a poner de manifiesto el riesgo de discriminación en el acceso a servicios por parte de los colectivos de mayores cuando el servicio únicamente se presta mediante versiones digitales que quedan fuera del alcance y competencia de ciertos colectivos de mayores.

También la DIT coordina y participa los webinarios desarrollados dentro de la cuarta temporada del **ciclo mujer y ciencia**, que se enmarca en el ámbito de las actividades de responsabilidad social de la AEPD y en el que se viene a poner de relieve el prestigio y liderazgo de la mujer en el ámbito de la ciencia y la tecnología y donde mujeres de reconocido prestigio cuentan su visión como profesionales con relación a la protección de datos personales. Durante esta cuarta temporada se desarrollaron las siguientes conferencias:

- **Monitorización autónoma y eficiencia energética: Innovación en emergencias y protección de datos, María Cristina Rodríguez Sánchez**
- **Toma el control de tus datos: Ciudadanía empoderada e informada para una datocracia de calidad, Alicia Asín**

También ha iniciado una nueva serie de artículos sobre recomendaciones culturales relacionadas con la protección de datos. En 2024 han sido publicados los siguientes:

- **Artículo de apertura**
- **1984**
- **Un mundo feliz**

La DIT realiza un intenso esfuerzo de formación, tanto interno a la AEPD, como externo. En cuanto a la formación interna, se han realizado las siguientes actividades:

- Curso de Responsabilidad Proactiva
- Curso de Ciberseguridad
- Curso Interno de Cifrado y Protección de datos.
- Curso Interno de IA y Protección de Datos
- Curso Interno Gestión identidad-Verificación edad
- Curso Interno de cookies
- Curso Interno Modelado de amenazas
- Curso UNED - Metodología, Diseño y Validación Práctica de modelos generativos.
- Máster RGPD

Con el objetivo del impulso de la protección de datos en sus aspectos tecnológicos para salvaguardar los derechos y libertades de las personas físicas en el ámbito del desarrollo de la economía digital, la DIT ha desarrollado y colaborado los siguientes foros:

- Europäischer Datenschutztag 2024 – Digitale Transformation–die Datenschutz-Zukunft gestalten
- Curso TIC de alta dirección del Int. Gutiérrez Mellado: Protección de Datos y Espacios de Datos
- Master de RTVE: Inteligencia Artificial
- APEP: Inteligencia Artificial
- Congreso nacional sector Contact Center
- RootedCon 2024
- Infors@lud 2024
- TechFest 2024
- UNESCO IA
- Mesa redonda Observatorio BIDA
- Jornada BIG DATA, IA Y SMARTCITIES - Ayto de Madrid
- GT Interministerial Dato – Anonimización
- Seminarios Fundación Hermes
- II Semana de IA de Sevilla
- Reunión de la Global PET Network
- Tutorización en el XXIX Curso Selectivo CSSTI
- Jornada El valor de los datos en el entorno digital de la Universidad de Alicante
- DICOPO AI and data regulation: between convergence and novel challenges
- Máster en Derecho Digital de la UN – Inteligencia Artificial

- Cursos de INAP – M. Política Territorial – M. Presidencia – Defensa – M. Transporte – Armada - Interior
- Curso de la Abogacía del Estado
- Curso RIPD sobre RGPD
- Privacy Talk de PrivacybyDesign Japón
- PDP Week 2024 Singapur – RoudTable - PETs
- DPA Xchange Session 2, “Data Anonymisation in ASEAN” - Singapur
- Curso UIMP “Nuevos retos para la protección de los derechos de las personas ante el impacto de Internet”
- Curso UNED 2024 Valencia Procedimientos de diseño, implementación y despliegue de sistemas de inteligencia Artificial de Alto Riesgo – Gobernanza
- Digital Enterprise Show 2024 – Málaga La Administración Pública y la IA en la educación, la privacidad y la ciberseguridad de los menores.
- Master UNED – Protección de Datos – Auditorías de Seguridad
- Curso INAP Especialista - Dimensiones de la responsabilidad activa, enfoque de riesgos, EIPD y gestión de brechas de datos personales
- ENISA AHWG PRIVACY MEETING - Presentation report: AEDP-ENISA event on Data Spaces 2023
- Curso Practicas maliciosas comerciales en Internet INAP asturiano
- Curso Secreto estadístico - Anonimización Ministerio Trabajo
- Intergrupo de infancia del Parlamento Europeo
- Global Age Assurance Standards Summit – Manchester
- International Age Assurance Working Group – APPA - Singapur
- Future of Privacy Forum – Europe Call en verificación de edad
- CIPL – entrevista sobre verificación de edad
- UTECA, IA y verificación de edad de menores
- IV Congreso Infancia, Familia y Capacidad
- IA en el sector educativo (INTEF)
- IA en el tercer sector
- Ciberseguridad en el sector salud

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

La AEPD ha venido desarrollando durante 2024 sus funciones consultivas conforme a lo dispuesto en los artículos 57.1.b) y e) del RGPD y 47 de la LOPDPGDD, que contemplan la promoción de "la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento" y el "facilitar información a cualquier interesado en relación con el ejercicio de sus derechos…"

El equipo de atención al ciudadano de la Subdirección General de Promoción y Autorizaciones, en desarrollo de estas funciones, ha dado respuesta en 2024 a 55.673 consultas de los ciudadanos, tanto escritas, formuladas a través de la sede electrónica, como de manera telefónica, o a través de atención presencial.

En todas las respuestas se ha procurado informar y sensibilizar a los **casi 60.000 ciudadanos que han consultado a la Agencia sobre sus derechos de protección de datos**, cómo ejercerlos y la posibilidad de formular reclamaciones; también se ha intentado facilitar la comprensión de los riesgos, las garantías y los derechos relacionados con los tratamientos de datos que les afectan.

Además de estas actuaciones consultivas, en este periodo de 2024, una importante aplicación tecnológica se ha consolidado como el refuerzo esencial de la promoción informativa personal de la Agencia: el ChatBot informativo que se inserta en la página de entrada en la web de la agencia como un icono de ayuda con un globo azul.

Se puso en marcha en abril de 2023 como un canal de atención continuada (24h x 7d) e inmediata a las dudas y preguntas más habituales. El nuevo canal de ayuda se presta a través de un mecanismo de Chatbot y ofrece la posibilidad de que, si no se encuentra la ayuda en la respuesta robótica, se deriva la consulta a un operador personal.

Los resultados del Chatbot en su primer año completo de funcionamiento han sido excelentes, arrojando unas cifras de 42.489 consultas al año y con un nivel de satisfacción reportado por los propios usuarios del 75%.

Toda la base del conocimiento del Chatbot ha sido preparada por el equipo de atención al ciudadano de la Agencia y se actualiza regularmente adaptándolo a los cambios normativos y de criterio que se producen.

Conviene subrayar que la actividad consultiva de la Agencia se ha incrementado en un 29% respecto al año anterior, lo que ha puesto de manifiesto el compromiso del equipo de atención al ciudadano para ayudar a los ciudadanos.

También, como en años anteriores, **se han actualizado las preguntas frecuentes** (FAQs, por su acrónimo inglés) publicadas en la web de la AEPD, con la finalidad de acercar y hacer más fácil y ágil el acceso de los ciudadanos a las cuestiones más demandadas en protección de datos, y se han añadido nuevas secciones a la lista, como, por ejemplo, una sección autónoma para facilitar el uso del Canal Prioritario.

Respecto de las materias objeto de consulta, a lo largo del año 2024 las consultas más frecuentes han sido las relacionadas con reclamaciones, seguidas por las consultas sobre la aplicación del Reglamento General de Protección de Datos y al ejercicio de los derechos de protección de datos. En este año cabe señalar un número importante de consultas referidas a la utilización del DNI, comunidades de vecinos, y también sobre llamadas publicitarias de comercializadores de energía aun en casos en los que los ciudadanos se encontraban en la lista de exclusión publicitaria.

Respecto de las quejas recibidas, 221, se observa lo siguiente:

- Una utilización inadecuada del formulario de queja, que se usa en algunos casos para comunicar la oposición o desacuerdo ante determinados tratamientos de datos: publicidad, spam, acoso publicitario, ficheros de morosos o cámaras de vídeo vigilancia. Se trata de "quejas" frente a la actuación de otros responsables o terceros, pero no relativas al funcionamiento de la Agencia. Estas mal llamadas quejas se canalizan y responden como consultas y computan a efectos estadísticos como consultas.

- También se han recibido quejas relacionadas con problemas de acceso a la web, y con la utilización de los formularios para interponer reclamaciones cuyo uso se puso en marcha este año.

- En el período de referencia, del total de los 221 registros presentados con formulario de queja, más de la mitad de ellas eran simplemente consultas.

3.1. Educación y menores

Las consultas se han categorizado según quién las formula o desde dónde, tal y como se ha realizado en las Memorias de años anteriores. Los canales habilitados por la AEPD para consultar cuestiones relacionadas con Educación y Menores son:

- Sede electrónica,
- correo de canaljoven@aepd.es,
- WhatsApp 616 172 204
- y teléfono 900 293 621.

La cifra de consultas recibidas y atendidas por el Área de Educación y Menores (Canal Joven) durante 2024, asciende a un total de 3.592

La mayoría de las consultas proceden de progenitores, el 55% del total, relacionadas mayoritariamente con los tratamientos de datos personales de sus hijos tanto en el ámbito educativo, en el que destacan las dudas sobre la utilización de plataformas educativas, como en el ámbito personal en relación con la publicación de imágenes de los menores por familiares o amigos en redes sociales. Otras consultas recurrentes son las relativas al tratamiento de datos de los menores en el ámbito deportivo, en especial la grabación y posterior difusión de imágenes mientras llevan a cabo prácticas deportivas.

En el ámbito educativo, agrupando las consultas realizadas tanto desde los colegios de educación primaria (CEIP) como los institutos de educación secundaria (IES) se llega al 8% del total, generalmente se plantean sobre tratamientos de datos personales del alumnado derivados de la captación y posterior difusión de imágenes en la web del centro o en perfiles de redes sociales.

En cuanto a las consultas que se realizan desde Universidades, el 1%, la mayoría están centradas en tratamientos de datos personales relacionados con los trabajos fin de grado (TFG) o fin de máster (TFM). Se constata que la gran mayoría de los profesores desconocen la figura del Delegado de Protección de Datos, obligatoria para las Universidades tanto públicas como privadas.

También se han recibido consultas de empresas privadas, un 6%, normalmente de empresas de ocio infantil, academias de idiomas o música, gabinetes de pedagogos/psicólogos que tratan datos personales de menores de edad. Sus consultas están relacionadas con la necesidad de conocer la normativa de protección de datos personales y la forma adecuada de su cumplimiento.

Las consultas de organismos públicos, un 5%, generalmente las realizan Entidades Locales sobre publicación de imágenes de menores en sus webs, recogidas durante eventos o fiestas populares organizadas por estas administraciones. También nos remiten consultas policías locales, relacionadas con actuaciones policiales en las que están involucrados menores de edad.

Otra categoría la conforman las consultas formuladas por el alumnado, un 3%, tanto de menores como de mayores de edad, en este último caso, fundamentalmente alumnos de universidades.

Sus consultas vienen motivadas en su mayoría por la información que sobre ellos los centros educativos y universitarios trasladan a sus progenitores, o bien por la publicación de calificaciones.

Por último, dentro de esta descripción de las consultas recibidas en 2024, conviene tener en cuenta que se han atendido numerosas consultas (21%) realizadas por ciudadanos que quieren reclamar el tratamiento de datos personales realizado tanto por empresas privadas como por Administraciones Públicas. Desde el Canal Joven se procura dar información precisa y detallada sobre los distintos modelos de reclamaciones.

Además de las consultas recibidas, cabe señalar que desde el Canal Prioritario de la AEPD que gestiona la Subdirección General de Inspección de Datos, se han derivado a Canal Joven a lo largo del 2024, un total de 27 reclamaciones que no cumplían los requisitos del Canal Prioritario para la retirada inmediata de contenido sensible, con el fin de que pudieran gestionarse como consulta y poder así dar información a los ciudadanos.

COLABORACIÓN EN ACTIVIDADES FORMATIVAS

- **Curso NOOC Menores y seguridad en la Red, 5ª edición**, realizada en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE) y el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF), con el objetivo de dar a conocer pautas, herramientas y estrategias tanto a familias como a profesionales de la educación que permitan evitar los riesgos de un uso inadecuado o poco seguro de la red de los menores de edad. Se matricularon más de 1.900 alumnos.

- **Curso MOOC, Promoviendo la ciberseguridad y privacidad desde la coordinación TIC, 1ª edición**, actividad formativa realizada en colaboración con INTEF e INCIBE, con el objetivo de ofrecer una visión general de las funciones que realiza la Coordinación TIC de los centros escolares en relación con la ciberseguridad y privacidad en el uso de la tecnología, la colaboración con otras figuras y equipos educativos, así como la dinamización de las competencias digitales asociadas entre el profesorado y el alumnado del centro educativo.

  Actividad dirigida a docentes que realicen labores de Coordinación TIC en su centro educativo o aquellos que se estén preparando para realizar esta función. Se matricularon más de 1.600 alumnos.

- **Curso Menores y Redes Sociales**, organizado en colaboración con la Fiscalía General del Estado, en el que se analizaron los problemas de salud derivados de un uso inadecuado de las redes sociales, así como las medidas posibles para limitar el acceso a las mismas por los menores y los medios para educarles en un uso sano de las mismas. Realizado en dos ediciones 19 y 20 de febrero.

Participación en Jornadas en el entorno educativo y de menores

Organizado por	Fecha	Denominación	Ponencia
Universidad de Murcia	8 de febrero	Jornada Protección de Datos y Menores (Murcia)	Líneas de acción de la AEPD para la protección de los menores en el entorno digital
Generalitat de Cataluña	21 de marzo	Jornada 'Cómo proteger a los niños, niñas y adolescentes del acceso a la pornografía en el ámbito digital' (Barcelona)	La legislación española sobre la protección de la infancia y la adolescencia
Secretaría de Estado de Seguridad (Min. Interior)	09 de abril 07 de mayo	II Jornadas Formativas sobre Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos	Protección del Menor en la Internet de las cosas
Asociación Aragonesa de delegados de protección de datos	16 de abril	III Jornadas Aragonesas de Protección de Datos, Transparencia y Ciberseguridad (Calatayud)	El móvil en las aulas
Consejería de Desarrollo Educativo y FP (Junta de Andalucía)	17 de junio	Jornada efectos negativos que las pantallas están teniendo en el desarrollo psicológico y social de la infancia y la adolescencia (Sevilla)	Privacidad y Salud Digital
Fundación Cursos de Verano de la Universidad del País Vasco	25 de junio	Curso de verano: Digitalización de la enseñanza: una visión desde la protección de datos (San Sebastián)	Privacidad y Salud Digital
Pantallas Amigas, Universidad de Deusto y Asociación de Internautas	27 de junio	Jornada Videojuegos y derechos digitales de la infancia (Bilbao)	Protección de los derechos de las personas menores en los entornos digitales desde la AEPD
Pantallas Amigas	7 de octubre	Jornada 'Inteligencia artificial y derechos de la infancia en el contexto digital'	Menores y derechos digitales
Universidad Rey Juan Carlos	8 de octubre	IV Congreso Internacional sobre Menores y medios sociales: identidades digitales vulnerables y controles de contenidos en salud emocional	Moderación, regulación y autorregulación en redes sociales y medios
Defensor del Pueblo Andaluz	9 de octubre	Jornada 'Derechos en Red. Por un espacio digital seguro para la infancia y adolescencia' (Cádiz)	Privacidad, Educación y Salud Digital
Fundación Atresmedia	19 de octubre	3er Encuentro para profesores Mentes AMI	La protección de los derechos digitales de niños y jóvenes

Organizado por	Fecha	Denominación	Ponencia
Asociación Multidisciplinar y de Investigación sobre la Infancia y Parentalidad Positiva (ASEMIP)	25 de octubre	IX Congreso ASEMIP 2024 'Infancia y parentalidad positiva: prevención de la violencia y Adicciones en línea' (Cuenca)	Conferencia de Clausura
Fundación Plan B y Ayuntamiento de Zamora	12 de noviembre	4ª Semana de la Infancia y la Adolescencia (Zamora)	Derecho del menor a la intimidad y protección de datos
INTEF	3 y 4 de diciembre	Congreso Nacional de Competencia Digital Educativa (Valladolid)	
Asociación Profesional Española de Privacidad (APEP)	12 de diciembre	La patria potestad digital y el acceso a los contenidos de los dispositivos digitales de los menores por parte de sus progenitores	

MATERIALES PUBLICADOS POR EL ÁREA DE EDUCACIÓN Y MENORES

https://www.tudecideseninternet.es/

- **Informe sobre responsabilidades y obligaciones en la utilización de dispositivos digitales móviles en la enseñanza infantil, primaria y secundaria**

FAQS PUBLICADAS EN APARTADO PREGUNTAS FRECUENTES

- **FAQ ¿Para la realización de actividades que implican contacto habitual con menores de edad, es obligatorio aportar un Certificado Negativo de Delitos de Naturaleza Sexual?**
- **FAQ ¿Pueden los centros educativos instalar sistemas de videovigilancia?**

DIFUSIÓN DE MATERIALES RELACIONADOS CON MENORES E INTERNET

- **Convocatoria de los Premios 2024 a las Buenas Prácticas Educativas en privacidad y protección de datos para un uso responsable y seguro de internet por los menores.** Tras la publicación de la resolución de la AEPD en el BOE el 31 de mayo de 2024, se difunde la información a colaboradores, Consejerías de Educación de las CC.AA., Delegados de Protección de Datos de las Consejerías de Educación de CC.AA., Asociaciones de Familias (CEAPA, CONCAPA…) desde el Canal Joven el 17 de junio.
- **Orientaciones sobre 'Responsabilidades y obligaciones en la utilización de dispositivos digitales móviles en la enseñanza infantil, primaria y secundaria'**, enviado el 23 de septiembre a las Autoridades autonómicas de Protección de Datos, Consejerías de Educación de las CCAA, así como a sus DPD, al Ministerio de Educación, Formación Profesional y Deporte y a las asociaciones de familias más representativas.

- **Difusión de la Actualización del Plan Digital Familiar de la Asociación Española de Pediatría (AEP)**, que incorpora contenidos del Informe del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia creado por el Consejo de Ministros, del que ha formado parte la Directora de la AEPD. Una de las medidas aprobadas por el Comité y propuestas al Gobierno ha sido el desarrollo de una regulación adecuada del uso de los dispositivos digitales en los centros educativos, que quede reflejada en sus Planes Digitales y que establezca límites a la digitalización de la enseñanza según la edad (incluyendo el tiempo de pantalla de las tareas que se realizan fuera del horario escolar) siguiendo las pautas fijadas por las sociedades científicas y teniendo en cuenta la política de protección de datos, de seguridad y privacidad.

  En este sentido, el 5 de diciembre de 2024, la Asociación Española de Pediatría ha actualizado estos criterios científicos y publicado las recomendaciones sobre los periodos diarios de uso de las pantallas, siguiendo el compromiso adoptado por el grupo de trabajo de Salud Digital del Comité de Promoción de la Salud de la AEP de revisar anualmente el contenido según la evidencia científica acumulada en el último año. Desde la AEPD se dio difusión a las Consejerías de Familia, Educación y Sanidad de las distintas CC.AA. el 18 de diciembre.

ACTUACIONES ESPECÍFICAS

- **Grupo de Trabajo 'Menores, Salud Digital y Privacidad'**, del que se mantuvieron dos reuniones. La primera el 11 de enero, donde cada una de las entidades participantes en el grupo planteó cuáles eran las MEDIDAS CONCRETAS a proponer, entre las que destacan: contar con un sistema de verificación de edad respetuoso con los derechos de los adultos; regulación del etiquetado de contenidos de los videojuegos, recomendaciones en el ámbito de la salud digital; impacto de las nuevas tecnologías en el neurodesarrollo, regulación de los neuroderechos, adopción de medidas legales para la protección de los menores en el sector digital; medidas en el ámbito educativo; formación de las familias; e impulso en las instituciones de la UE de proyectos para la defensa de los menores en el ámbito digital.

  En la segunda reunión, que tuvo lugar el 5 de febrero, se siguió ahondando en las medidas a tomar y se planteó desde la AEPD la necesidad de modificar la LOPDPGDD para incrementar de 14 a 16 años la edad mínima de consentimiento en el ámbito de la protección de datos.

- **Presentación de la estrategia reforzada sobre 'Menores, salud digital y privacidad' el 29 de enero.** Establece 3 ejes, estratégicos, 10 actuaciones prioritarias y 35 medidas.

- **Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia creado por el acuerdo de Consejo de Ministros de 30 de enero de 2024.** Activa participación de la Directora en condición de experta en todas las reuniones del comité. El informe del comité se presentó por la Ministra de Juventud e Infancia al Consejo de Ministros el 3 de diciembre de 2024. El informe incluye un diagnóstico de la situación referida a la protección de la juventud y la infancia en el ámbito digital y la propuesta al Gobierno de 107 medidas para su estudio, agrupadas en tres bloques temporales de implantación (corto, medio y largo plazo). El objetivo es que las Administraciones Públicas garanticen un marco de prevención, detección precoz y protección frente a una posible vulneración de los derechos de la infancia y la adolescencia.

- **Actualización web Canal Joven https://www.tudecideseninternet.es/**, durante el segundo semestre del año, para renovar la información contenida y desarrollar un entorno más amigable que pueda servir de contacto a la AEPD con el público más joven y su entorno.

Valoración candidaturas Premios Buenas Prácticas Educativas 2024, por parte del equipo de la unidad de Educación y Menores se ha llevado a cabo la valoración de las candidaturas presentadas a los Premios 2024 Buenas Prácticas Educativas, Modalidad A y B, revisando 12 y 9 candidaturas respectivamente.

REUNIONES

- Autismo España, 7 de febrero
- Fundación Cibervoluntarios, 7 de marzo
- DigitalES, Ametic y fabricantes de Dispositivos, 16 de abril
- Youforget it, 23 de abril
- Pantallas Amigas, 25 de abril

3.2 Comunicación

Las iniciativas llevadas a cabo por la Agencia en 2024 han motivado un amplio número de acciones de comunicación con el objetivo de ampliar su difusión entre los colectivos destinatarios de estas. A continuación, se recogen las acciones relacionadas con el departamento de prensa y comunicación:

3.2.1 Redes sociales

La Agencia ha continuado difundiendo materiales y consejos **a través de su perfil en la red social X (antes Twitter), con más de 800 mensajes publicados en 2024. Se superaron los 39.000 seguidores**.

Los tuits más destacados los siguientes: los anuncios de las medidas cautelares contra Worldcoin y las funcionalidades electorales de Meta, diferentes contenidos acerca del Canal prioritario e información acerca de la responsabilidad de las familias por los actos cometidos por sus hijos e hijas en Internet.

En cuanto a **LinkedIn**, se ha convertido en 2024 en el perfil de la Agencia en redes sociales **con más cuentas alcanzadas e interacción de los usuarios**.

Los temas son comunes con los que la Agencia aborda en otras redes sociales, pero las características de esta red social permiten explicar los asuntos que se difunden de forma más detallada. **El perfil ha aumentado en más 7.500 los seguidores en 2024, alcanzando casi los 25.000, con más de 200 post publicados** (que fueron vistos por más de un millón y medio de usuarios de LinkedIn) y más de 90.000 interacciones. Así, se realizaron más de 400 comentarios, casi 7.000 usuarios compartieron los posts en su perfil de LinkedIn y pincharon en los enlaces de los posts en más de 57.000 ocasiones.

Los temas con más reacciones que se publicaron en el perfil de LinkedIn son los siguientes: los contenidos publicados con motivo del día de la protección de datos; la medida cautelar impuesta a Worldcoin; información sobre el consentimiento para tratar datos personales de personas menores de edad y contenidos acerca de los derechos recogidos en la normativa de protección de datos.

Por otro lado, la Agencia sigue trabajando en la realización de contenidos para **Instagram**, una red social con la que este organismo trata de dar a conocer los derechos y las obligaciones de protección de datos a un público que no tiene por qué estar especializado en estas cuestiones.

Durante 2024, en el perfil de la Agencia en Instagram **más de 65.000 usuarios vieron publicaciones de la AEPD**, siendo las publicaciones más vistas las campañas 'Hay más riesgos en Internet que en la vida real' y 'No a la barra libre digital', acciones que por su importancia se analizan en un apartado específico de esta Memoria. Asimismo, en esta red social también hay que destacar la publicación del Decálogo sobre el impacto de la pornografía en niños, niñas y adolescentes. Como se puede observar en la comparativa entre unas redes y otras los contenidos más vistos difieren

entre unas y otras, debido al tipo de público que compone la propia red social.

En 2024 la Agencia también se ha seguido trabajando en el perfil de **YouTube**, con más de 250.000 reproducciones de los vídeos del canal y se han publicado 13 vídeos nuevos.

Este canal engloba cuatro tipologías de vídeos: la grabación de presentaciones, 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. Los contenidos más vistos durante 2024 en YouTube están relacionados con las campañas 'No a la barra libre digital' y 'Hay más riesgos en Internet que en la vida real', y la configuración de las opciones de privacidad en redes sociales como X y LinkedIn.

3.2.2 Otras acciones de difusión

3.2.2.1 Boletín informativo mensual AEPD

La Agencia ha mantenido durante 2024 un boletín informativo mensual que tiene como destinatarios principales a las entidades adheridas al Pacto Digital, las personas delegadas de protección de datos registrados en la Agencia y las personas y/o entidades que se han inscrito específicamente para su recepción. El objetivo del mismo es agrupar los lanzamientos y novedades de la Agencia orientadas fundamentalmente a responsables de tratamiento, aunque también recoge temas diversos centrados en la ciudadanía.

El boletín se publica también en la web, lo que permite consultarlo de forma retroactiva y bajo demanda. También funciona como una herramienta de comunicación interna, ya que se envía a todo el personal de la Agencia para reforzar el conocimiento de las novedades sobre las acciones realizadas. En diciembre de 2024 se envió el número 29 de esta newsletter.

3.2.2.2 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, analizar el impacto de las nuevas tecnologías emergentes en la privacidad y para hacer pedagogía del derecho fundamental a la protección de datos personales.

Durante 2024 el blog de la Agencia ha recibido **más de un millón de visitas únicas**, con un importante crecimiento respecto a 2023.

Entre los posts que han despertado un mayor interés se encuentran los relacionados con la difusión de vídeos con contenido violento en redes sociales; los riesgos del sharenting; brechas de datos personales; la identidad como derecho, y si los colegios pueden tomar imágenes del alumnado durante las actividades escolares.

Además, en cuanto a contenidos hay que destacar que este año se puso en marcha una nueva sección dentro del blog de la Agencia **orientada a realizar recomendaciones sobre referencias culturales**, que se han destacado en su análisis de la privacidad desde diferentes puntos de vista.

Así, se han difundido creaciones cuya temática profundiza en los derechos y libertades de las personas, entendiendo que esta referencia atañe principalmente a los derechos a la protección de datos y a la intimidad.

3.2.2.3 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 la ciudadanía 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 viernes 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 241 piezas temáticas.

3.2.2.4 Relaciones con los medios

La difusión de los derechos y obligaciones en materia de protección de datos que realizan los medios de comunicación es un elemento de gran relevancia en dos de las funciones encomendadas a la Agencia: promover tanto la sensibilización de la ciudadanía y la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de sus datos personales, como la de los responsables en el adecuado cumplimiento de la normativa.

A lo largo de 2024, 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 la gestión de casi un centenar de entrevistas, tribunas o artículos de análisis y el envío proactivo de notas de prensa a medios y a los departamentos de comunicación de las organizaciones adheridas al Pacto Digital. Estas notas se publican también en la página principal de la Agencia, habiendo recibido casi un millón y medio de visitas.

Entre las notas de prensa más consultadas en 2024 se encuentran las vinculadas a la utilización de datos biométricos para el control de presencia y acceso; la estrategia global sobre menores, salud digital y privacidad; la guía sobre el uso de cookies con adaptación a las directrices del Comité Europeo de Protección de Datos; la propuesta de sistema de verificación de edad para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet; la medida cautelar impuesta a Worldcoin; las orientaciones sobre las obligaciones por el uso de dispositivos móviles en los centros docentes o el informe sobre la influencia de los patrones adictivos en Internet, y en especial sobre los menores de edad.

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) y con noticias enviadas para su publicación en la web del CEPD.

3.3 Agenda institucional

Durante 2024 la Agencia continuó participando en numerosas reuniones, jornadas, foros, congresos, cursos, seminarios web, actos y presentaciones, tanto como entidad organizadora o invitada. El objetivo es tanto difundir las acciones e iniciativas realizadas por la Agencia como promover el conocimiento de la normativa de protección de datos. La relación completa de la agenda institucional de la AEPD puede consultarse en **esta sección web**. En relación con este apartado, se incluye también una tabla detallada en la sección de La Agencia en cifras 'Atención al ciudadano y sujetos obligados'.

Cabe destacar la firma de los Protocolos Generales de Actuación con:

- El Instituto de Mayores y Servicios Sociales (IMSERSO), el 16 de enero, con la voluntad de reforzar el compromiso para una protección más eficaz del derecho a la privacidad en el marco de la protección de datos en colectivos vulnerables.

- La Universidad de Castilla-La Mancha (UCLM), el 25 de octubre, con el objetivo de fijar un marco de actuación común para avanzar en el conocimiento técnico-científico de los derechos digitales en los entornos laborales y empresariales y, en especial, en relación con el derecho a la protección de datos personales de las personas trabajadoras en los lugares de trabajo, así como de las mejores prácticas existentes respecto de ello que redunden en beneficio de los derechos y libertades de las personas en el tratamiento de sus datos personales, fundamentalmente mediante el fomento de la colaboración, la generación y divulgación de conocimiento y la formación de profesionales.

Además, se han firmado adendas de prórroga de los protocolos existentes con la Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA), la Fundación Mutua Madrileña y la Fundación ANAR (Ayuda a niños y Adolescentes en Riesgos).

3.4 Presentaciones

Las acciones de divulgación realizadas por la Agencia también incluyeron en 2024 la presentación de diversas iniciativas con presencia de medios:

- **Presentación de la Estrategia de la AEPD sobre menores, salud digital y privacidad (29 de enero)**

  Con motivo de la celebración del Día Internacional de Protección de Datos, la Agencia presentó su **Estrategia global sobre menores, salud digital y privacidad**, un documento que recoge sus líneas de actuación prioritarias para fomentar la protección efectiva de la infancia y adolescencia en el uso que realizan de Internet y sus servicios. La apertura del evento corrió a cargo de la Agencia y la CNMC, y contó con las intervenciones del presidente del Gobierno, Pedro Sánchez, y la ministra de Infancia y Juventud, Sira Rego.

- **Entrega de los Premios Protección de Datos 2023 (29 de enero)**

  El mismo día de la presentación de la Estrategia de menores, salud digital y privacidad de la AEPD se entregaron los '**Premios de Protección de Datos 2023**', que reconocen los trabajos que promueven en mayor medida la difusión y el conocimiento del derecho a la protección de datos como su aplicación práctica. Tanto la presentación completa de la Estrategia como el acto de la entrega de premios **pueden verse aquí**. Además, respecto de los premiados, se realiza una difusión específica de su trabajo a través de redes sociales.

- **Medida cautelar Worldcoin (6 de marzo)**

  La Agencia realizó una presentación a los medios de comunicación para anunciar que había ordenado una medida cautelar contra Tools for Humanity Corporation para que cesase en la recogida y tratamiento de datos personales que estaba realizando en España en el marco de su proyecto Worldcoin, tras las numerosas informaciones publicadas por estos medios y la alarma social en torno a estas actividades. Esta decisión se basó en circunstancias excepcionales, adoptando medidas provisionales dirigidas al cese inmediato de ese tratamiento de datos personales, prevenir su posible cesión a terceros y salvaguardar del derecho fundamental a la protección de datos personales.

- **Curso Universidad Internacional Menéndez Pelayo 2024 (10-12 de julio)**

  La Agencia impartió el curso **Nuevos retos para la protección de los derechos de las personas ante el impacto de Internet**, enmarcado en las Actividades de Verano 2024 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander. El curso se inició presentando un informe que analiza cómo los tratamientos de los datos personales de los usuarios en numerosas plataformas, aplicaciones y servicios incluyen patrones adictivos para aumentar su tiempo de conexión. Tras la presentación del informe se celebró una mesa redonda centrada en la salud digital y privacidad de la infancia y adolescencia, así como diversas ponencias acerca del control de la edad para el acceso a las plataformas digitales, las actuaciones que ha llevado a cabo la Agencia para promover su protección o la experiencia del Parlamento Europeo. La segunda jornada abordó la Inteligencia Artificial y su relación con la protección de datos personales, así como la neurotecnología, neurodatos y neuroderechos. Por último, durante la tercera de las jornadas se impartieron conferencias sobre los servicios digitales en la Unión Europea, los desafíos del Comité Europeo de Protección de Datos o el Marco de Privacidad UE–EEUU, entre otros temas.

- **Balance Responsabilidad Social 2019-2014. Medidas de protección a la infancia y adolescencia en el entorno digital (16 de diciembre)**

  La Agencia presentó un balance de las principales acciones puestas en marcha en los últimos años para la protección de la infancia y adolescencia en el entorno digital, entre las que se incluyó un informe que explica cómo la exposición prolongada a patrones adictivos y engañosos puede ser perjudicial para la salud, y en especial, para los más jóvenes. El secretario de Estado del Ministerio de Juventud e Infancia, Rubén Pérez Correa, que clausuró el evento, abogó por un cambio de paradigma para que los entornos digitales sean espacios seguros donde niños, niñas y adolescentes vean garantizados sus derechos. Seguidamente, se celebró una mesa redonda dedicada a la protección de la infancia y adolescencia en el mundo online con la participación de la pediatra coordinadora del grupo de trabajo de salud digital de la Asociación Española de Pediatría (AEP), María Salmerón; el decano-presidente del Colegio Oficial de la Psicología de Madrid, José Antonio Luengo; el responsable de Educación y Derechos de la Infancia de UNICEF España, Nacho Guadix, y la presidenta de la Asociación de Adolescencia Libre de Móviles de Madrid (ALMMA), María Gijón.

3.5. Iniciativas de colaboración y difusión

3.5.1 Jornada de formación para institutos

La AEPD participó en el webinario 'Jóvenes, móviles y violencia de género', organizado por la Fundación Mutua Madrileña y Antena 3 Noticias mediante su iniciativa 'Contra el maltrato, Tolerancia Cero', y dirigido a todos los institutos y centros de Educación Secundaria de España.

La intervención de la Agencia estuvo centrada en ofrecer claves para contribuir a la salud digital de la adolescencia, abordando, entre otros aspectos, la prevención del ciberacoso o la difusión de contenido sexual o violento, así como soluciones prácticas como el Canal prioritario.

El acto fue grabado en el colegio Menesiano de Madrid y retransmitido en abierto desde jovenescontraelmaltrato.com, y estuvo conducido por la periodista y presentadora de Antena 3 Noticias, Victoria Arnau, contando también con la participación de la agente del Cuerpo Nacional de Policía, Vanessa Gil, y la creadora de contenidos, Andrea Garte.

Más de 10.000 estudiantes de Secundaria siguieron en directo el webinar sobre jóvenes y móviles.

3.5.2 Actualización de los vídeos Protege tu privacidad: X y LinkedIn

Tras la actualización en 2023 de los vídeos de configuración de la privacidad y seguridad de **Instagram**, **Tik Tok** y **Whatsapp**, la Agencia renovó en junio de 2024 los videotutoriales de **X** y **LinkedIn**. Los vídeos se inician con una breve introducción explicando qué es y para qué se utiliza cada servicio. A continuación, realizan un tutorial que guía a los usuarios paso a paso a través de las opciones de configuración de privacidad y seguridad de cada uno de ellos, ofreciendo recomendaciones para optar por el mayor grado de privacidad posible.

3.5.3 Colaboración con la asociación Dale Una Vuelta y el Colegio Oficial de Psicología de Madrid

La Agencia colaboró en el **decálogo sobre el impacto de la pornografía en niños, niñas y adolescentes** junto a la asociación Dale Una Vuelta y el Colegio Oficial de Psicología de Madrid, alertando de los riesgos que produce la visualización precoz de pornografía en la infancia y adolescencia.

3.5.4 Colaboración con la Asociación Española de Psiquiatría de la infancia y la adolescencia

La Asociación Española de Psiquiatría de la infancia y la adolescencia (AEPNYA) presentó un informe sobre los riesgos asociados al uso de tecnologías. La Agencia colaboró en la difusión del mismo, englobándose estas acciones en el fomento de la colaboración activa con entidades y dentro de su Estrategia Global sobre menores, salud digital y privacidad.

3.5.5 Colaboración en el Día Mundial de Internet

La AEPD, como parte del Comité de Impulso del Día de Internet y que está compuesto por 62 colectivos sociales, participó un año más en las reuniones preparatorias del #diadeinternet 2024. Estas abarcaron, entre otros asuntos, la elección del tema central de la edición, la elaboración del 'Manifiesto por una Inteligencia Artificial comprometida con las personas' para su posterior lectura durante el XVIII Congreso de Editores CLABE.

3.5.6 Quinta edición del curso online "Menores y seguridad en la Red", organizado por la AEPD, INCIBE e INTEF

La Agencia, el Instituto Nacional de Ciberseguridad (INCIBE) y el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF) lanzaron la **5ª edición del curso online gratuito 'Menores y seguridad en la Red'**, que tuvo lugar del 31 de enero al 9 de febrero. La Agencia contribuyó a la difusión del curso a través de su web de menores, sus redes sociales y su blog.

3.5.7 Primera edición del curso online 'Promoviendo la ciberseguridad y privacidad desde la coordinación TIC', organizado por la AEPD, INCIBE e INTEF

La Agencia, el Instituto Nacional de Ciberseguridad (INCIBE) y el Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado (INTEF) lanzaron la 1ª edición del curso online "Promoviendo la ciberseguridad y privacidad desde la coordinación TIC", celebrado del 9 de abril al 21 de mayo. Como en el anterior, la AEPD contribuyó a su difusión.

3.6 Campañas de difusión

‘No a la barra libre digital’

La Agencia y la Fundación Atresmedia se unieron para alertar sobre los peligros del acceso de los menores a contenidos inadecuados a través del móvil y promover el acompañamiento en el uso de la tecnología en la infancia y adolescencia. Esta campaña recomienda a las familias que retrasen la entrega del móvil a sus hijos e hijas y los acompañen en su interacción con el mundo digital, evitando así que accedan a contenidos inapropiados y perjudiciales para su desarrollo, como contenidos pornográficos o violentos, entre otros.

‘No a la barra libre digital’ refuerza la idea de que permitir a los menores el acceso temprano y sin restricciones a las pantallas es abrir la puerta a riesgos que pueden impactar en su bienestar. Así, el spot visualiza esta problemática a través de imágenes impactantes: un niño solo en una barra americana y una niña en un local de apuestas, acompañadas de un mensaje claro y directo: “**Si no dejarías que tu hijo o hija estuviese solo en un sitio como este…, tampoco le dejes solo frente al mundo digital. Retrasa la entrega del móvil a tus hijos e hijas y acompáñalos en su uso**”.

La campaña comenzó a emitirse el 14 de noviembre bajo el hashtag #Noalabarralibredigital, y se difundió en todos los canales de televisión del Grupo Atresmedia: Antena 3, la Sexta, Nova, Neox, Mega y Atreseries, y en sus soportes multimedia, así como en la página web y redes sociales de la AEPD y la página web y las redes sociales de la Fundación Atresmedia.

‘Hay más riesgos en Internet que en la vida real’

La Agencia y el Consejo General de la Psicología de España (COP) lanzaron la campaña ‘Hay más riesgos en Internet que en la vida real’, orientada a que las familias valoren las consecuencias de entregar a sus hijos e hijas un dispositivo con acceso a todo tipo de servicios de Internet. La campaña contó con la colaboración de Atresmedia, Mediaset España y RTVE, que se comprometieron a la difusión en sus respectivos canales, reforzando así su compromiso en la difusión de los derechos de la infancia y adolescencia en el entorno digital.

Con la campaña '**Hay más riesgos en Internet que en la vida real**', la AEPD y el COP quieren invitar a las familias a reflexionar sobre qué supone realmente hacer entrega de un smartphone a sus hijos e hijas, **equiparando los efectos de determinados servicios de Internet a la dependencia y adicción que generan algunas sustancias**.

A menudo, las familias no han recibido información y no son conscientes en toda su dimensión de los efectos que produce en niños, niñas y adolescentes el uso inadecuado o problemático y adictivo de ciertos servicios de Internet, afectando gravemente a su desarrollo personal, y en concreto a su salud (física, mental, psicológica y social, sexual); su neurodesarrollo; su aprendizaje; las relaciones familiares y sociales; los hábitos de consumo, o la monetización de sus datos.

Asimismo, el lanzamiento de esta campaña de la Agencia junto al COP profundiza en la **Estrategia global sobre menores, salud digital y privacidad de la AEPD**.

'Contra el maltrato: Tolerancia Cero'

La Agencia participó en un vídeo enmarcado en la campaña de la Fundación Mutua Madrileña y Atresmedia 'Contra el maltrato: Tolerancia Cero'. En ella se difunde el Canal prioritario indicando la forma de solicitar la eliminación de imágenes, vídeos o contenido sensible (sexual o violento) que pueda perjudicar a una persona.

Contra el Maltrato, Tolerancia Cero se proyecta más allá de la televisión, ya que llega a más de 400 municipios que se han sumado a la iniciativa 'Municipios Contra el Maltrato'. Asimismo, la Agencia también colaboró con la Fundación Mutua Madrileña y Atresmedia en la II Jornada de formación online con institutos de toda España y en la I Mesa de Expertos Tolerancia Cero, con el objetivo de analizar la violencia y el maltrato que se manifiesta también en el mundo online.

3.7. Premios

3.7.1 Premios concedidos por la AEPD

La Agencia hizo públicos el 25 de enero de 2024 los nombres de los galardonados con los '**Premios Protección de Datos 2023**', que reconocen en diferentes categorías los trabajos que promueven tanto la difusión y el conocimiento del derecho a la protección de datos como su aplicación práctica.

Los premios se otorgan en las categorías: Comunicación; Proactividad y buenas prácticas en el cumplimiento del Reglamento y la LOPDGDD; Buenas prácticas educativas; Investigación 'Emilio Aced'; Emprendimiento 'Ángela Ruiz Robles'; Buenas prácticas para la protección de las mujeres frente a la violencia digital, y Difusión del derecho a la protección de datos en redes sociales.

En la categoría de **Comunicación**, la AEPD concedió el premio a la **Fundación Maldita.es**, por su trabajo 'Nuevos retos de la inteligencia artificial y la protección de datos: un enfoque multiformato para abordar debates actuales y futuras dudas', que incluye una cobertura dedicada a explicar cómo la inteligencia artificial puede afectar a la ciudadanía y, en concreto, a la protección de datos personales.

Respecto al **Premio a la Proactividad y Buenas Prácticas en el cumplimiento del Reglamento Europeo de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los derechos digitales**, en la modalidad de empresas, asociaciones y fundaciones, el jurado concedió el premio al **Instituto de Salud Global de Barcelona (ISGlobal)**, por 'Cultura institucional en materia de protección de datos personales. Un enfoque integrador'. Este trabajo representa un ejercicio de buenas prácticas en investigación biomédica, ofreciendo un enfoque global y desarrollando herramientas de difusión complementadas con formación.

En la modalidad de entidades del sector público se otorgó el premio, ex aequo, a la **Delegación de Protección de Datos de la Generalitat Valenciana**, por sus 'Recomendaciones para la protección de datos de las mujeres víctimas de violencia de género y otros tipos de violencia en su relación con la Administración de la Generalitat y su sector público instrumental', un proyecto dirigido a los centros sociales, sanitarios y de justicia donde se atiende a mujeres víctimas de violencia de género y otros tipos de violencia.

Este premio, ex aequo, también se concedió al **Grupo de trabajo para la protección de datos personales de la Comunidad de Madrid**, adscrito a la Secretaría General Técnica de la Consejería de Presidencia, Justicia y Administración Local de la Comunidad de Madrid, por su 'Difusión y concienciación de la Protección de Datos Personales en la Administración de la Comunidad de Madrid', una iniciativa que, por una parte, proporciona a los trabajadores información sobre protección de datos de la Administración de la CAM con un lenguaje sencillo y comprensible y, por otra, muestra a los ciudadanos sus derechos de una forma clara, directa y cercana.

Igualmente, fue galardonada, ex aequo, la **Diputación de Segovia**, por su 'Plan de Asistencia en materia de Protección de Datos Personales para los Municipios de la provincia de Segovia con población inferior a 20.000 habitantes', un proyecto que incluye distintas acciones para fomentar una cultura de protección de datos entre los empleados públicos de las entidades locales de la provincia y que contempla la puesta a disposición de la ciudadanía de folletos y carteles informativos sobre cómo se protegen sus datos en su ayuntamiento.

En la categoría de **Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet por los menores**, el jurado concedió el premio en la modalidad dirigida a centros de enseñanza de Educación Primaria, ESO, Bachillerato y Formación Profesional, al **CEIP Villafría de Otero** (Asturias) por su proyecto 'En Villafría, dejamos las pantallas y vivimos la vida', que fomenta el uso responsable de los dispositivos y promueve actividades como la firma de un contrato familiar o la elaboración de un juego para poner en práctica actividades que faciliten la desconexión.

En la modalidad de compromiso de personas, instituciones, organismos, entidades, organizaciones y asociaciones, públicas y privadas, se otorgó el premio, ex aequo, a la **Asociación Española de Pediatría**, por su **Plan Digital Familiar**, una iniciativa que ofrece pautas avaladas por la evidencia científica para aprovechar las ventajas de la tecnología reduciendo los riesgos sobre la salud de los menores, con recomendaciones adaptadas a las circunstancias de cada familia.

Dentro de esta modalidad, el jurado también premió a la **Asociación Dale una Vuelta**, por '**Generación XXX**', una campaña de concienciación sobre el uso responsable y seguro de internet por los menores que se centra en el peligro que supone el acceso a la pornografía, al tiempo que alerta de la necesidad de un sistema de verificación de edad para acceder a esos contenidos.

Además, resultó premiada la **Unidad de C1B3RPOLICÍA de la Policía Local de Rincón de la Victoria (Málaga)**, por 'El Municipio ante la Protección de Datos Personales y la Privacidad en los Menores', un proyecto local con actividades de formación y concienciación para fomentar un uso responsable de internet por los menores a través de charlas, talleres en centros escolares y formación de los profesionales.

En la categoría de **Investigación en protección de datos personales Emilio Aced**, el jurado concedió el premio a Yod Samuel Martín García, por su trabajo 'Contribuciones desde la ingeniería de software y sistemas basada en modelos a la privacidad y la protección de datos mediante un enfoque multidisciplinar'. Este proyecto plantea abordar las cuestiones de privacidad y protección de datos desde el inicio del desarrollo de un sistema y, en particular, integrar la privacidad y la protección de datos en la ingeniería de software y

sistemas, en aspectos como la gestión de riesgos, la ingeniería de requisitos, el diseño o el aseguramiento de sistemas e ingeniería de métodos.

Respecto a la categoría de **Emprendimiento en protección de datos personales Ángela Ruiz Robles**, el jurado premió a **Internxt Universal Technologies**, por 'Internxt, proyecto que fomenta la creación de un Internet respetuoso y seguro', que aborda los desafíos relacionados con la encriptación postcuántica, la categorización avanzada de datos y las técnicas de procesamiento del lenguaje natural, poniendo de relieve la importancia de salvaguardar la privacidad en un entorno digital en constante evolución.

En la categoría de **Iniciativas y buenas prácticas para una mayor protección de las mujeres frente a la violencia digital**, el jurado premió a la **Fundación ANAR**, por 'La violencia contra las mujeres no tiene edad', una campaña compuesta por un spot y una serie de vídeos formativos destinada a concienciar a menores, familias y docentes sobre qué es la violencia de género y cómo prevenirla.

Finalmente, en la nueva categoría de **Difusión del derecho fundamental a la protección de datos en redes sociales**, el jurado otorgó el premio a **Eduard Blasi Casagran y Elena Gil González**, por su perfil Tech and Law en **Instagram** y **TikTok'**, que ofrece contenido sobre derecho digital y novedades tecnológicas de forma sencilla y comprensible, tanto para la ciudadanía como para profesionales de la protección de datos.

Asimismo, ha concedió un accésit, ex aequo, a **Elena y Laura Davara Fernández de Marcos**, por 'Legado familiar Davara: De cuando no existían las redes y ya divulgaba la importancia de la privacidad al uso de las redes sociales como vía de difusión del derecho de protección de datos', compuesto por tres perfiles –**dos** en **Linkedin** y uno en **Instagram**– que contribuyen a la difusión entre los ciudadanos de los principios de este derecho y fomentan la concienciación entre los responsables del tratamiento.

Finalmente, el jurado también otorgó este premio, ex aequo, a **F. Javier Sempere Samaniego**, por su 'Crossover entre el RGPD y la LOPDGDD. The perfecto mix v.3.0', que conjuga **un perfil en X** que lleva más de una década difundiendo contenidos relacionados con la protección de datos personales, con un completo documento que cruza los artículos del RGPD y sus considerandos con los respectivos de la LOPGGDD.

3.7.2 Premios recibidos por la AEPD

En 2024 la Agencia Española de Protección de Datos fue galardonada con un total de siete premios, que forman parte de los 36 que la Agencia ha recibido en los últimos años por las acciones realizadas para proteger a las personas en un mundo digital.

★ **'Mejor iniciativa en materia de Ciberseguridad, privacidad y protección de datos en el ámbito sanitario' de los Premios Nacionales de Informática de la Salud 2023.**

La AEPD ha sido galardonada por la Sociedad Española de Informática de la Salud (SEIS) en la categoría de 'Mejor iniciativa en materia de Ciberseguridad, privacidad y protección de datos en el ámbito sanitario' en sus Premios Nacionales 2023 por el proyecto impulsado por la División de Innovación Tecnológica de la Agencia '**Criterios de verificación para proteger a los menores de edad ante el acceso a contenidos para adultos en Internet**', "atendiendo a la necesidad incipiente de controlar el acceso de menores a contenido no apropiado y especialmente por el alto impacto que tiene en el desarrollo de los menores el consumo de contenido inapropiado".

★ **Premio QIA a la innovación en el sector público.**

La Agencia Española de Protección de Datos ha obtenido el Premio internacional de la 17ª edición de los Quality Innovation Award (QIA), en la categoría Innovación en el sector público, por su proyecto 'Iniciativas prácticas para proteger a los menores en internet con entornos saludables, positivos y seguros'. La organización de los Premios QIA ha considerado el proyecto de la Agencia como una quality innovation a nivel internacional, una innovación que cumple con cinco características: novedad, utilidad, aprendizaje, orientación al cliente y efectividad.

★ **Premio 'Ciberseguridad de los datos' de los Premios Socinfo Digital Revista Sociedad de la Información Digital.**

La Agencia Española de Protección de Datos ha sido galardonada por la Revista Sociedad de la Información Digital en la categoría 'Ciberseguridad de los datos' de los Premios Socinfo Digital – Ciberseguridad AAPP por su iniciativa 'Proyecto de verificación de edad para la protección del menor ante el acceso a contenidos de adultos en Internet'. El objetivo de estos premios es divulgar proyectos de desarrollo de las TIC en las Administraciones Públicas aplicadas en los servicios al ciudadano y a la mejora de la eficacia interna.

★ **Premio Proyecto Público del Consejo General de Colegios Profesionales de Ingeniería Informática de España.**

La Agencia Española de Protección de Datos ha resultado premiada por el Consejo General de Colegios Profesionales de Ingeniería Informática de España (CCII) en la categoría 'Proyecto Público', por su **sistema de verificación de edad para la protección del menor ante el acceso a contenidos de adultos en Internet** y, en especial, por "la puesta en marcha de un proyecto que permite proteger a un colectivo con mayor vulnerabilidad de una serie de riesgos que pueden encontrarse mientras navegan en la red".

★ **Premio @aslan 2024 en la modalidad de Servicios al Ciudadano.**

La Agencia Española de Protección de Datos ha sido galardonada en los Premios @aslan 2024 en la modalidad de 'Servicios al Ciudadano', por su **sistema de verificación de edad** para proteger a los menores de edad ante el acceso a contenidos de adultos en Internet.

★ **Premio 'Innovación' de los Global Privacy and Data Protection Awards 2024.**

El sistema de verificación de edad propuesto por la Agencia Española de Protección de Datos (AEPD) para proteger a la infancia y adolescencia en Internet fue galardonado en la categoría de 'Innovación' de los **Global Privacy and Data Protection Awards 2024**, concedidos en el marco de la 46ª Asamblea Global de Privacidad, que reúne a más de 140 autoridades de protección de datos y privacidad a nivel mundial. Estos premios tienen como objetivo reconocer la excelencia y la innovación de las buenas prácticas puestas en marcha por las Autoridades.

★ **Premio 'People's Choice' (Premio del Público) de los Global Privacy and Data Protection Awards 2024.**

El sistema de verificación de edad propuesto por la Agencia Española de Protección de Datos (AEPD) para proteger a la infancia y adolescencia en Internet fue galardonado en la categoría de 'People's Choice' (Premio del Público) de los **Global Privacy and Data Protection Awards 2024**, concedidos en el marco de la 46ª Asamblea Global de Privacidad. El Premio del Público se elige a su vez entre los ganadores de las cuatro categorías que engloban estos galardones, resultando la AEPD ganadora asimismo del Premio a la 'Innovación'.

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

3.8 Acceso a la información pública y transparencia

La transparencia, en sus dos vertientes (publicidad activa y atención a las solicitudes de acceso a la información pública), es uno de los pilares en los que se asienta la independencia de esta Agencia en el desarrollo de las funciones que tiene encomendadas.

En cuanto a la transparencia activa, la AEPD publica de manera periódica y actualizada a través de su propia **Página Web**, toda la información institucional, organizativa, de planificación, de relevancia jurídica, económica, presupuestaria y estadística que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG) establece. A lo largo de 2024 se han realizado 259.245 visitas a la página web de la AEPD.

En cuanto al acceso a la información pública, se aprecia un aumento en el número de solicitudes, pasando de las 112 recibidas en 2023 a las 158 de 2024, lo que manifiesta un creciente interés por parte de los ciudadanos, por conocer cómo funciona esta autoridad de control.

La mayor parte de las solicitudes, como en ejercicios anteriores, piden acceso a expedientes correspondientes a procedimientos de inspección, así como a informes jurídicos y otros documentos elaborados por la AEPD. Junto con estos, también han sido objeto de petición de información las retribuciones del personal de la Agencia, la notificación de brechas de seguridad e informaciones relativas a evaluaciones de riesgo de tratamientos de datos personales.

Como demostración del compromiso que la AEPD tiene con la sociedad en materia de transparencia, como ya hizo en 2023, ha emitido el 100% de las resoluciones de acceso dentro del plazo legalmente establecido para resolver. Además, todas las resoluciones firmes denegatorias, o parcialmente denegatorias, de acceso a la información pública, se publican en la Página Web de la AEPD para el mejor conocimiento de la motivación de las actuaciones en el ámbito de la transparencia.

De las 157 solicitudes de acceso a la información pública que han sido resueltas a lo largo de 2024, 16 han sido reclamadas frente al Consejo de Transparencia y Buen Gobierno (CTBG); tan solo una de ellas ha sido estimada por el Consejo.

Cabe destacar por su interés general, la resolución del CTBG que da la razón a la AEPD. En ella el CTBG resuelve que la AEPD actuó correctamente al denegar el acceso a unas actuaciones realizadas por no tener el solicitante la condición de interesado y por encontrarse el procedimiento en la fase de actuaciones previas. Consideró el CTBG procedente la denegación de la agencia de acuerdo con el artículo 14.1.e) de la LTAIBG, cuya finalidad es garantizar el correcto desarrollo de todos los actos de investigación practicados en la fase de instrucción de un procedimiento penal, administrativo o disciplinario, y reconociendo que existe un riesgo cierto de que las diligencias se vean afectadas por la divulgación de la información.

Asimismo, en otra resolución, el CTBG ha confirmado la decisión de la AEPD de inadmitir de conformidad con el artículo 18.1.c) de la LTAIBG, una solicitud de acceso que exigía la selección de las resoluciones sancionadoras relacionadas con un determinado tema, la extracción de las fechas y la elaboración de un resumen de las mismas, entendiendo que esto equivalía a solicitar la confección de un informe “ad hoc” de acuerdo con los criterios definidos por el solicitante. Todo ello, teniendo en cuenta que la totalidad de las resoluciones sancionadoras de la AEPD se encuentra publicada en su página web, en la que es posible realizar búsquedas en función de distintos conceptos.

De especial interés, también, la resolución en la que el CTBG afirma que el derecho a la información pública no ampara la pretensión de revisar las resoluciones dictadas por esta Agencia.

La UIT de la AEPD es, además, el punto de contacto nacional para las solicitudes de acceso a información del Comité Europeo de Protección de Datos.

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.

A nivel nacional, participa en el grupo de trabajo que reúne a todas las UIT de la Administración General del Estado, convocado y dirigido por la Dirección General de Gobernanza Pública del Ministerio para la Transformación Digital y de la Función Pública.

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 o micro empresas, en las mismas condiciones que se establecen para los DPD.

Las **consultas recibidas** en este año ascienden a un **total de 724**, y se observa una ligera disminución, en torno al 10%, respecto de las consultas de DPDs formuladas el año pasado. Sin embargo, se observa una **mayor la complejidad de las consultas**.

En cuanto a su contenido, se pueden resaltar como más relevantes, las siguientes:

En el ámbito de la seguridad pública:

Continúa el interés, como en años anteriores, por las cuestiones relacionadas con la videovigilancia y con la interpretación de 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. Se han generado importantes dudas respecto de la normativa aplicable a la instalación de videocámaras fijas en la vía pública por las Fuerzas y Cuerpos de Seguridad del Estado. En estas cuestiones la AEPD, junto al resto de autoridades autonómicas, ha interpretado que la exigencia de autorización para la instalación de videocámaras fijas establecida por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su normativa de desarrollo continúa vigente, no habiendo sido derogada por la Ley Orgánica 7/2021, de 26 de mayo.

En el ámbito laboral:

Continúan siendo frecuentes las consultas sobre la implantación de sistemas biométricos como medida para el control horario de los trabajadores y el control de acceso. Sobre estas cuestiones ha tenido especial incidencia la publicación de las "Directrices 05/2022 del CEPD sobre el uso de técnicas de reconocimiento facial en el ámbito de aplicación de la ley", que pone de manifiesto que con la evolución tecnológica resulta necesario establecer mayores controles, tanto para la autentificación como para la identificación en base a elementos biométricos de la persona, y que deben plantearse los límites al tratamiento de datos biométricos, así como las medidas que han de establecerse para que un tratamiento de datos personales que decida utilizar sistemas biométricos garantice el cumplimiento RGPD. Sobre estas cuestiones la AEPD ha publicado una **Guía sobre tratamientos de control de presencia mediante sistemas biométricos** estableciendo los criterios para la utilización de la biometría en el registro de la jornada laboral o el control de acceso con fines laborales y no laborales.

En relación con la identificación requerida para registrarse en establecimientos de hostelería y el uso del DNI:

Durante 2024 se han formulado varias consultas de los responsables de establecimientos de hostelería y solicitando la opinión de la AEPD en relación con la nueva normativa al respecto, el Real Decreto 933/2021, con ocasión de su aplicación durante este año 2024.

En relación con el sector de hostelería:

Se remitió una nota informativa, sobre el uso de sistemas o cámaras de videovigilancia, a la Confederación Española de Hoteles y Alojamientos Turísticos (CEHAT) y a la Confederación Empresarial de Hostelería de España (CEHE).

4.2 Delegados de Protección de Datos

La función de Delegado de Protección de Datos (DPD) representa un elemento fundamental para el cumplimiento del RGPD tal y como se pone de manifiesto tanto en el RGPD como en la LOPDGDD, donde se establecen con detalle las funciones, posición y características que este rol debe desempeñar con el fin de asesorar al responsable del tratamiento en el cumplimiento de las obligaciones que dicha normativa le impone.

La AEPD ha continuado impulsando la puesta a disposición de las personas que desempeñan esta función de herramientas, recursos y canales de comunicación con el fin de que puedan desempeñar su función con las mayores garantías de solvencia e independencia. Al mismo tiempo, la AEPD ha continuado también con la labor de concienciación a los responsables obligados a la designación de DPD, así como los que consideren su designación de forma voluntaria, a fin de dotar a esta figura de recursos suficientes para el desarrollo de las tareas que el RGPD le atribuye.

Ya en 2023 la AEPD participó en la acción europea coordinada para analizar la designación y situación de los delegados de protección de datos en entidades públicas y privadas, dentro del marco de actuaciones coordinadas del CEPD. Dicha acción ha dado como resultado un informe que ofrece una visión tanto del sector público como privado con el fin de contribuir a elevar el nivel de cumplimiento y la protección de los datos personales de los ciudadanos en el conjunto de la Unión Europea.

Durante 2024 la AEPD también ha participado en la acción coordinada dirigida a analizar la práctica de la atención del ejercicio del derecho de acceso en la que las personas que desempeñan la función de DPD desempeñan también un papel destacado tanto en el asesoramiento a los responsables, como en el diseño, puesta en práctica y revisión de los procedimientos que las organizaciones utilizan para la atención efectiva de estas solicitudes. Para ello, la AEPD ha contado con la colaboración de los DPD de organismos del sector público, así como de entidades del sector privado en los ámbitos del transporte aéreo de viajeros, comercio, asegurador, financiero, seguridad privada, energético, turismo y hostelería, comunicaciones, farmacéutico y de ensayos clínicos.

El informe final recoge recomendaciones y puntos de atención dirigidas a los responsables y a las autoridades de control relativas a la identificación de retos y puntos de mejora; identificación de buenas prácticas, necesidad de definir procedimientos internos así como uso de plataformas para la gestión de la privacidad; utilización de los canales adecuados para la presentación de solicitudes; medidas de protección e identificación de los interesados; así como la necesidad de incrementar el nivel de concienciación dentro de las organizaciones en relación con el ejercicio de los derechos de las personas interesadas.

4.3. Certificación del DPD conforme al esquema AEPD-DPD

En aplicación del artículo 39 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, es necesario que la designación de los Delegados de Protección de Datos (DPD) se produzca atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su artículo 35, establece que la cualificación profesional que se exige podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación.
A tal fin, la Agencia Española de Protección de Datos (AEPD), elaboró en julio de 2017 un Esquema de Certificación.

En 2024 las principales magnitudes de dicho Esquema tienen que ver con el número de DPD certificados, que han sido 206, el 53.8% de los 83 candidatos a obtener la certificación en un total de 72 convocatorias.

El número total de DPD que han obtenido la certificación con arreglo al Esquema de la AEPD a 31 de diciembre de 2024 **asciende a 1.306**.

El número de DPDs que ha sido comunicados a la AEPD en total es de 11.227, que prestan servicio a 119.803 responsables del tratamiento, si bien se muestra que el porcentaje de Dpd certificados sobre el total de DPD's continúa aumentando, llegando a 11,63% (10,52% el año anterior). Este año 2024 ha sido en el que más DPD's se han certificado de los últimos 5 años.

En cuanto a las entidades de formación, dos universidades se han interesado por el reconocimiento de su formación por la AEPD, y les han sido facilitados los formularios para que soliciten dicho reconocimiento, si lo estiman de su interés y sus programas se adaptan al Esquema, si bien todavía no han presentado solicitud formal.

4.4 Códigos de conducta

El RGPD proporciona un conjunto de instrumentos que permiten a las organizaciones gestionar sus obligaciones en materia de protección de datos y demostrar su cumplimiento, entre ellos, los códigos de conducta.

Establece el RGPD que se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta dentro de los límites fijados por el Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas concernidas.

Desde la AEPD, a través de la Subdirección de Promoción y Autorizaciones, se han venido promoviendo reuniones con aquellos sectores que se puedan beneficiar de la tramitación y aprobación de códigos de conducta que respondan a las necesidades específicas en materia de protección de datos, fomentado activamente la elaboración de dichos proyectos de códigos, tratando de resolver las dudas de interpretación y 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.

Asimismo, y en cumplimiento de lo establecido en la Disposición transitoria segunda LOPDPGDD, se continua con el proceso de adaptación de los códigos tipo.

En algunos supuestos, y tal como se ha realizado en ejercicios anteriores, se ha solicitado la colaboración de otras unidades de la AEPD en aquellos apartados que tratan materias que conforman su trabajo diario.

Asimismo, la Agencia Española de Protección de Datos, siguiendo la línea marcada por el Comité Europeo de Protección de Datos y a la vista del número cada vez más alto de denuncias en materia de protección de datos, ha promovido la adopción en los códigos de conducta de procedimientos extrajudiciales de resolución de conflictos que permitan resolver de manera rápida y satisfactoria las reclamaciones de los sujetos titulares de los datos. Con este fin, desde la Subdirección de Promoción y Autorizaciones se ha realizado un gran esfuerzo que se ha visto reflejado no sólo en los códigos de conducta que tienen como contenido básico el establecimiento de un procedimiento de mediación, sino también en la inclusión de dicho mecanismo en los códigos de conducta, aprobados por la AEPD, cuyo contenido fundamental es la regulación de tratamientos u operaciones de tratamiento de datos.

En el año 2024 la AEPD ha aprobado un código nacional, y ha participado como autoridad corredactora del Dictamen de la Comisión de aprobación de un código trasnacional. Por otra parte, la AEPD ha cancelado la inscripción de cuatro códigos tipo, por falta de adecuación al RGPD (DT2 LOPDPGDD).

Actualmente se encuentran en distintas fases de tramitación **ocho proyectos** de códigos de conducta, de los cuales 5 son referidos a adaptación de códigos tipo y uno es un código de conducta. El resto de los códigos de conducta en tramitación son transnacionales.

Asimismo, hay **10 iniciativas** de códigos de conducta nacionales.

CÓDIGOS DE CONDUCTA NACIONALES

El total de códigos aprobados por la AEPD son los cuatro en que se relacionan a continuación:

'Código de conducta de tratamiento de datos en la actividad publicitaria' promovido por AUTOCONTROL, aprobado en 2020 y que ha sido modificado en el año 2023, para adecuarlo a los cambios normativos de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones y de la LOPDPGDD, así como a lo dispuesto en la Circular de la AEPD 1/2023 de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

'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 FARMAINDUSTRIA, y aprobado por la AEPD el 10 de febrero de 2022.

'Código de conducta regulador del tratamiento de datos personales en los sistemas comunes del sector asegurador' promovido por UNESPA y aprobado el 29 de junio de 2022.

'Código de conducta para la resolución de controversias de protección de datos en el sector de las comunicaciones electrónicas', promovido por GRUPO ORANGE: Orange Espagne, S.A.U. Orange España Virtual, S.L. GRUPO TELEFÓNICA: Telefónica de España, S.A.U. Telefónica Móviles España, S.A.U. GRUPO VODAFONE: Vodafone España, S.A.U. Vodafone ONO, S.A.U. GRUPO MÁSMÓVIL: Xfera Móviles, S.A.U. Euskaltel, S.A.U. R Cable y Telecable Telecomunicaciones, S.A.U. y Pepemobile, S.L. Este código se aprobó de la AEPD de 17 de octubre de 2024.

En todos estos códigos la resolución de aprobación incluye la acreditación de los organismos de supervisión correspondientes.

Conforme al el punto 6.1 de los Criterios de acreditación para los organismos de supervisión de códigos de conducta, se han recibido los informes de actividades correspondientes a los tres códigos aprobados con anterioridad al año 2024, habiéndose procedido a su análisis para verificación del cumplimiento de lo establecido en los mismos.

CÓDIGOS DE CONDUCTA TRANSNACIONALES

Además, la AEPD ha participado en la tramitación de proyectos de códigos de conducta liderados por autoridades de protección de datos de otros Estados miembros en el marco del procedimiento coordinado.

En el ejercicio 2024, la AEPD ha actuado 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).

Asimismo, la AEPD ha participado como autoridad corredactora del Dictamen 12/2024 sobre el proyecto de Decisión de la Comisión Autoridad de Supervisión en relación con el **'Código de Conducta para la Prestadores de Servicios en Investigación Clínica'** presentado por EUCROF.

Por último, hay que señalar que se han mantenido numerosas reuniones online y presenciales con el CEPD, en el Subgrupo de Cumplimiento, Gobierno electrónico y Salud, en las que se han debatido entre otros temas el Código de EFPIA, el Código de EUCROF, el Código de WADA (antidopaje) y se ha participado en las reuniones ad hoc con el equipo de redacción de las **Directrices sobre el tratamiento de datos personales con fines de investigación científica**.

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 en general, que incluye la explicación 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.

La AEPD ofrece **dos modalidades** de cursos:

- Curso de 20 horas, configurado en 8 ponencias e impartido en modalidades online o presencial.

- Curso de 6 módulos en formato Moodle. Se ha incorporado la realización de una videoconferencia en directo, en cada uno de los módulos, para una mayor interacción entre alumnos y profesorado.

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 2024 se ha dirigido a:

- La Administración General del Estado: Ministerios de: Sanidad; de Transportes y Movilidad Sostenible; Interior; Trabajo y Economía Social; Política Territorial y Memoria Democrática; Presidencia, Justicia y Relaciones con las Cortes; Defensa.

- 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 en dos ediciones al año, que han contado con 600 alumnos.

- En este marco hay que destacar el "Programa especializado para DPD de las administraciones públicas", curso específico para formar a los futuros DPD y cuya edición, con nueva metodología y estructura, se impartió a 80 alumnos durante el primer semestre del año.

Se ha participado en esta l**abor de promoción y sensibilización** en los siguientes cursos y/o eventos:

- Jornada "Protección de datos personales en las entidades sociales" organizado por Plataforma de ONG de Acción Social.

- "Direct-Your Digital Rights", promovido por JEF Spain.

- VI Curso de Especialización en Servicio Exterior en la Escuela Diplomática del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

- "Gestión y automatización de solicitudes de acceso del interesado", en ISMS Forum.

- Jornadas de Concienciación Regional sobre la Protección de Datos en el Sector Salud (Costa Rica), organizado por FIIAPP.

- El DPO como pieza clave de los nuevos equipos de gestión de datos. Jornada APEP.

- Farmaforum 2024, por León research S.L.

- Curso acceso escala titulados superiores de OO.AA. organizado por el Ministerio de Industria y Turismo.

- Jornada sobre protección de datos organizada por el Centro de Referencia Estatal de Atención al Daño Cerebral (CEADAC).

- Webinar Legal Innovation Days, organizado por Wolters Kluwer Legal Sotfware.

- Diálogo Político de Alto Nivel en protección de Datos, de FIIAPP.

- Jornada de seguridad de la información y protección de datos, organizada por la Guardia Civil.

- XXVI Jornada Internacional de Seguridad de la Información de ISMS Forum.

- Máster de la Universidad Complutense de Madrid sobre Transparencia y Buen Gobierno.

- Curso selectivo de la 46ª promoción de Letrados de la Administración de Justicia, organizado por el Centro de Estudios Jurídicos del Ministerio de Presidencia, Justicia y Relaciones con las Cortes

Jornadas organizadas en la AEPD:

- Curso Menores y Redes Sociales, dirigido a Fiscales. Organizado con la Fiscalía General del Estado y el Centro de Estudios Jurídicos, 19 y 20 de febrero.
- II Sesión Informativa con alumnos de la facultad de Derecho de Stetson University, Florida, sobre protección de datos personales en el ámbito laboral.
- Sesión sobre implicaciones del GDPR para las empresas estadounidenses y nuevo marco para las transferencias internacionales de datos, impartida a alumnos de la Universidad de Suffolk, Boston.
- Visita del Instituto de Acceso a la Información Pública de Honduras (IAIP) el 25 de noviembre de.2024. Visita de carácter informativo.
- Visita de la Comisión Nacional de la Protección de datos de Marruecos, 3 de diciembre 2024. Visita de carácter informativo
- Jornada 'Cinco años de Responsabilidad Social y Protección de la Infancia y la Adolescencia en el entorno online', 16 de diciembre.

Un aspecto importante en el ámbito de la promoción es el conjunto de actividades que se dirigen 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 2024 se ha intervenido en las siguientes jornadas organizadas por:

- Red Iberoamericana de Protección de Datos (Costa Rica).
- Ayuntamiento de Bormujos (Sevilla).
- Policía Nacional.
- Instituto de las Mujeres (Mº de Igualdad) y Universidad de Salamanca.
- Consejo General del Poder Judicial, Gobierno Vasco y Universidad de Deusto.
- Delegación del Gobierno en la Comunidad Autónoma de las Illes Balears Balears.
- Ayuntamiento de Iznalloz (Granada).

4.6 Transferencias internacionales

Durante 2024 la AEPD ha aprobado las normas corporativas vinculantes (BCR por sus siglas en inglés) promovidas por los grupos multinacionales de Telefónica, Mapfre, FCC y Avature, una vez que el Comité Europeo de Protección de Datos emitió las correspondientes opiniones favorables durante su tramitación en el marco del procedimiento coordinado y consistencia previsto en el RGPD.

El total de BCR adoptadas por la AEPD a finales de este período es de 16, encontrándose en distintas fases de tramitación 5 proyectos de BCR en el marco del citado procedimiento coordinado.

Además, la AEPD ha participado como autoridad co-revisora en la tramitación de 4 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

El año 2024 ha venido marcado, tecnológicamente, por la irrupción de la inteligencia artificial y su integración en gran parte de aplicaciones de la vida cotidiana de los ciudadanos: desde asistentes virtuales de las grandes empresas tecnológicas o las recomendaciones personalizadas de las plataformas de películas, música o productos; hasta aplicaciones de salud y bienestar o de banca y finanzas. Esto viene a sumar todavía mayor presencia, alcance y complejidad a los tratamientos de datos personales en la sociedad actual y se refleja en la preocupación de los ciudadanos por la privacidad de sus datos personales y a su vez en el registro de reclamaciones ante la Agencia, que **este año 2024 ha sido el segundo más alto en la línea histórica**, solo por detrás del 2023, y un 25% superior a las recibidas en el año 2022.

Ante la creciente entrada de reclamaciones en los últimos años, la Agencia ha estado desarrollando distintas estrategias para hacer frente al trabajo entrante y así evitar el desbordamiento y el consiguiente colapso que se podría producir.

Una de las vías de abordar y plasmar estas estrategias ha sido la implantación de un **buzón de reclamaciones** en la sede electrónica de la AEPD. Este buzón, diseñado durante 2023 y en funcionamiento durante 2024, tiene por objetivo guiar y orientar a los ciudadanos para facilitarles la información sobre las circunstancias necesarias y la documentación mínima a aportar. Mediante una serie de preguntas y formularios, permiten saber si el conflicto planteado puede ser resuelto en el ámbito competencial de la Agencia, y de ser así, indica los distintos documentos e información necesarios para que la reclamación quede completa y pueda prosperar.

En una primera etapa de funcionamiento del buzón, se puso el foco en las reclamaciones recibidas con relación a la recepción de publicidad no deseada, dado su fuerte incremento en los últimos años y en especial en 2023, en que entró en vigor la nueva redacción de las garantías sobre las llamadas comerciales introducida en el artículo 66 de la nueva Ley General de Telecomunicaciones (LGTel). El resultado de la implantación del buzón ha llevado a que, mientras que en el año 2023 las reclamaciones de publicidad supusieron un 20% del total de reclamaciones de ese año, en 2024 han supuesto únicamente el 7% de las reclamaciones totales recibidas y sitúan a la publicidad en un cuarto puesto en cuanto a las reclamaciones más numerosas por categoría. Este descenso obedece a varios factores, pero de forma importante al buzón de reclamaciones, que permite además una mejora de la pertinencia y de la calidad de las reclamaciones presentadas, que ahora cuentan con la documentación mínima necesaria para poder ser tramitadas de manera efectiva.

Tras la publicidad, se ha habilitado también el buzón para las principales categorías de reclamaciones como son las de videovigilancia y las reclamaciones sobre ejercicio de derechos de protección de datos. En estas dos clasificaciones los resultados del buzón guiado por el momento no son tan visibles como en publicidad en cuanto a la reducción de las reclamaciones recibidas, pero sí en cuanto a su calidad, recibiéndose con las evidencias necesarias para su tramitación.

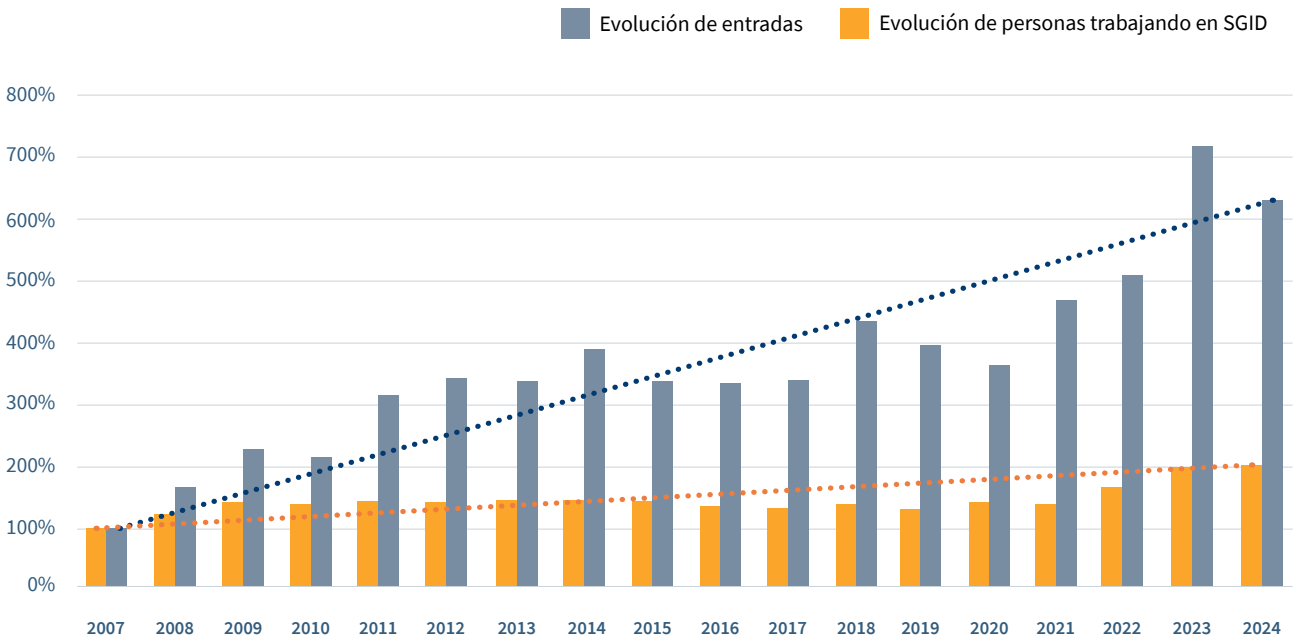
Puede decirse, por tanto, que la implantación del buzón guiado en la sede de la Agencia está dando sus frutos. Y no sólo por el número de reclamaciones recibidas, sino por la tasa de inadmisiones a trámite tras el análisis previo de la reclamación. Para que las reclamaciones puedan prosperar, deben superar primero un análisis para verificar que cumplen con los requisitos de admisibilidad establecidos en la normativa. Este año 2024 la tasa de inadmisibilidad se ha reducido un 9% gracias a la mejora de calidad de las reclamaciones recibidas a través del buzón guiado, que presentan la información mínima necesaria para poder ser admitidas y aportan la documentación que permite apreciar indicios racionales de la existencia de una infracción en el ámbito competencial de la Agencia.

Otro de los pilares en los que se basan las estrategias de la Agencia para hacer frente al creciente trabajo de los últimos años es la **adecuación del personal de la SGID**. Esta tarea se centra, fundamentalmente, en la creación de nuevas plazas y en el esfuerzo por tratar de cubrirlas mediante la búsqueda de talento. El leve crecimiento de 2024, de 103 hasta 106 personas, resulta de la creación de plazas aprobadas el año anterior, puesto que la previsión de creación de plazas en 2024 no ha sido posible llevarla a cabo dada la falta de presupuestos generales del Estado.

En el gráfico siguiente se compara el ritmo de crecimiento del personal, frente al de las reclamaciones entradas análogas que generan nuevos expedientes.

Estas entradas son mayoritariamente reclamaciones ante la AEPD, pero también casos recibidos de otras autoridades del espacio europeo, del canal prioritario de menores, notificaciones de brechas de seguridad en las que se abre investigación, y otros casos abiertos por propia iniciativa.

Evolución compatariva del nº de entradas y del personal de la SGID, 2007- 2024



La tasa de resolución de las reclamaciones ha sido del 96%. Es decir, se reciben más reclamaciones de las que la Agencia ha podido resolver en el año. Este factor ha aumentado ligeramente con respecto al año anterior (recordemos que 2023 fue el año en el que más reclamaciones se recibieron en la historia de la AEPD). Al resolverse un número menor de reclamaciones de las recibidas, como resultado el número de reclamaciones pendientes al finalizar el año ha aumentado. Esto pone de manifiesto que el crecimiento sostenido en la carga de trabajo no está encontrando respuesta en crecimiento de personal, como muestra con claridad la gráfica anterior, a lo que se añade que las reclamaciones recibidas son más pertinentes y a su vez, de una mayor complejidad fruto del mayor alcance de los tratamientos de datos personales.

Está complejidad está patente en que muchos casos investigados tienen un público potencialmente afectado muy amplio, debido a que las deficiencias se encuentran en los procedimientos de tratamientos de datos personales y no en casos particulares. La falta de un correcto diseño de estos procedimientos, adaptado a la normativa, hace que a raíz de una o varias reclamaciones relacionadas con un hecho aparentemente aislado, termine evaluándose la manera de proceder general del responsable para evitar que pueda albergar un potencial riesgo para la globalidad de sus clientes o usuarios de sus servicios.

Además, este incremento en la complejidad y alcance de los casos puede verse en otros aspectos varios de la tramitación. En primer lugar, y quizá el más indicativo, es el aumento de los tiempos medios de resolución en la mayoría de los procedimientos y actuaciones iniciados en la Subdirección General de Inspección de Datos o SGID, pero especialmente en las actuaciones previas de investigación, y en todos los procedimientos: derechos, sancionadores y apercibimiento.

Las **actuaciones previas de investigación** son las que determinan las circunstancias de la infracción y completan la identificación del responsable, y se realizan de forma potestativa con carácter previo al inicio de un procedimiento. Precisamente en los últimos años se han estado revisando los criterios que aconsejan su apertura, de manera que los inspectores puedan dedicar más tiempo a las investigaciones de los casos más complejos y de mayor impacto, y se puedan reducir las investigaciones que terminan en las que no se encuentran indicios de infracción. El tiempo medio de tramitación de estas investigaciones se ha incrementado en un 20% y más de la mitad de los casos (53%) han culminado en la apertura de un procedimiento tras corroborar que se había cometido una infracción. O lo que es lo mismo, estos dos últimos años ha mejorado la eficacia de las actuaciones al terminar menos investigaciones en archivo.

Algo similar sucede con los **procedimientos**: se han abierto un 10% menos que el año pasado y el tiempo de tramitación de los mismos se ha visto incrementado en un 25% de media, hecho que profundiza en la complejidad de los casos y de las tramitaciones que requieren.

Por último, de los procedimientos sancionadores finalizados en el año 2024, 281 impusieron una multa al responsable, frente a los 367 del año anterior.

Es decir, la Agencia ha interpuesto un 23% menos de número de multas. Sin embargo, el importe total de las mismas es mayor en casi un 20%, y la multa media se eleva a aproximadamente 125.000 €, un 56% más que en el año 2023.

Esto es **otro reflejo más de la mayor complejidad, alcance e importancia de los casos tratados**, que responde al cada vez mayor uso de datos personales y a su penetración en los diferentes ámbitos de la sociedad.

Continuando con las multas, en este año 2024 tres sectores han copado el 60% del importe total de las sanciones. Se trata de los **sectores suministro de agua y energía, entidades financieras y de crédito, y servicios de internet**. De entre ellos, hay 10 multas que tienen un importe superior al millón de euros. La **multa más grande** interpuesta en el 2024 le corresponde a ENERGYA VM GESTIÓN DE ENERGÍA, S.L. con un importe de 5 millones de euros por las infracciones de los artículos 5.1.a) y 5.2 del RGPD. **Le sigue otra multa** de 4 millones de euros interpuesta a GENERALI ESPAÑA, S. A. DE SEGUROS Y REASEGUROS por una quiebra de seguridad en la que se infringen los artículos 5.1.f), 32, 25 y 35 del RGPD. Puede leerse más sobre las mayores multas en el Anexo de "**La Agencia en cifras: Inspección de datos**" y sobre los casos más relevantes en el siguiente punto: **5.2 Reclamaciones y procedimientos más relevantes**

Precisamente, un ejemplo concreto que muestra la necesidad de salvaguardar la seguridad de los datos personales en los procesos de tratamiento, así como el riesgo que conlleva la falta de medidas que garanticen esta seguridad, son las **brechas de datos personales**. Los expedientes tratados en la AEPD que guardan relación con brechas de seguridad han tenido una presencia significativa tanto en el 2024 como en el 2023. Estos casos pueden llegar a conocimiento de la Agencia bien como notificaciones por parte de los propios responsables, de acuerdo con la obligación regulada en el artículo 55 del RGPD, bien como resultado de la recepción de reclamaciones por parte de los ciudadanos que se han visto afectados por ellas. En los dos últimos años, estas vías de entrada han dado lugar a importantes procedimientos que se inician con actuaciones previas de investigación y continúan, si así se determina, con un procedimiento sancionador.

En el pasado año 2024 el importe de las multas con las que se ha sancionado este tipo de infracciones supera los 13.000.000 €, valor casi similar al del año 2023. En conjunto, estos 26M€ suponen el 40% del importe total de multas interpuesto en los dos últimos años.

Otra vía de entrada de reclamaciones a la AEPD es a través de otras autoridades de control de los Estados del E**spacio Económico Europeo (EEE)**, dentro del ámbito de los mecanismos de cooperación recogidos en el RGPD. Este tipo de entradas permanecen al alza con un aumento del 17% con respecto al año anterior. Según el papel que desempeñe la AEPD como autoridad de control, estos casos pueden seguir diferentes caminos: pueden ser casos que no afecten ni puedan afectar potencialmente a ciudadanos españoles, ni el responsable tenga establecimientos en España, en cuyo caso España se declara no interesada y se archivan; pueden ser casos en los que España actúa como autoridad interesada, haciendo seguimiento de los avances, colaborando si fuera necesario con las otras autoridades y participando de forma activa en la decisión final adoptada; o España puede actuar como autoridad principal en aquellos casos en los que el responsable tenga su establecimiento principal en terreno nacional, llevando a cabo en estos casos la investigación y proponiendo una resolución que tiene que ser de mutuo acuerdo con el resto de autoridades de control interesadas.

A su vez, España debe mandar al resto de autoridades de control todas aquellas reclamaciones de ciudadanos españoles cuyo responsable tenga su establecimiento principal en otro Estado del EEE. En estos casos, la AEPD permanece como autoridad interesada y actúa de interlocutor entre el reclamante y la autoridad de control extranjera, participando además en la decisión final que se adopte.

Los casos transfronterizos, aunque muy inferiores en número a las reclamaciones locales, requieren de gran esfuerzo y son, en líneas generales, más prolongados en el tiempo. Además del intercambio inicial de la reclamación y la información y documentación pertinente, luego suponen un intercambio de mensajes en el que se coopera entre autoridades solicitando información, intercambiando información para los reclamantes y consensuando una resolución. En general el número de solicitudes y comunicaciones intercambiadas ha aumentado en torno a un 15%, destacando el número de casos que España ha compartido con otras autoridades y las solicitudes de asistencia en el marco de estos casos. Han disminuido los proyectos de decisión compartidos por parte de España con otras autoridades de control en los casos en los que España actuó como autoridad principal, no obstante, se corresponde con la media de casos liderados por España en los últimos años.

En el ámbito europeo, la SGID ha participado en varios grupos de trabajo 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 de la 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.

En el marco de las evaluaciones Schengen 2021-2025, se han llevado a cabo auditorías sobre grandes sistemas de información de la UE como son el Sistema de Información de Visados (VIS), el Sistema de Información Schengen (SIS II) o el EURODAC. De este modo, sobre el VIS, se han realizado entre otras inspecciones en el Consulado General de España en Argel, en el Consulado General de España en Manchester, en la Dirección General de la Policía o en la Jefatura Superior de Policía del País Vasco. En relación con el SIS II, se han realizado inspecciones, entre otros, a la Policía Nacional o al centro de procesado de datos de la Secretaría de Estado de Seguridad, responsable nacional del sistema SIS. Por último, en 2023 se incluyó al listado un nuevo gran sistema de las infraestructuras europeas: EURODAC. Durante 2024 se ha realizado una auditoría inicial de cumplimiento del sistema en lo referente a protección de datos, así como una auditoría anual a los accesos que utilizan huellas dactilares.

En este contexto, también se han mantenido reuniones de coordinación de SIS II y VIS con las autoridades nacionales respectivas para evaluar los resultados de los informes de evaluación, las medidas a adoptar por los distintos organismos y el calendario de implementación de estas. En este nuevo 2025 se harán los informes finales de las evaluaciones Schengen 2021-2025.

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 base de legitimación cuando pueden causar un perjuicio irreparable en el afectado. El número de entradas recibidas por este canal se mantiene en línea con los números del año previo. Sin embargo, no todas estas entradas se tramitan como urgentes pues primero tienen que pasar un análisis previo para determinar si efectivamente se trata de casos que requieren una actuación prioritaria y urgente. El número de entradas que sí se han tramitado por la vía preferente es un 34% superior a la del año pasado. Entre estas entradas también se incluyen reclamaciones ordinarias que se decide tramitar por la vía urgente.

La eficacia de las intervenciones realizadas en el ámbito de estos casos, medida por la proporción de retiradas de contenido requeridas y las efectivamente cumplidas en el año ha sido de un 82%, inferior a la de los años previos que superaban el 90%. Denota la dificultad de garantizar un cumplimiento de la normativa en un ámbito global como es Internet, especialmente cuando los prestadores de contenidos se encuentran fuera de España. Sin embargo, cabe destacar que el número de intervenciones realizadas se ha incrementado un 70% en línea con el incremento de casos tratados de manera urgente.

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**".

5.2 Reclamaciones y procedimientos más relevantes

La categoría de videovigilancia ha sido el grupo de actividad que ha supuesto un mayor número de reclamaciones durante 2024, con un 18% de las reclamaciones totales presentadas.

Dentro de los procedimientos de videovigilancia podemos destacar el **PS/00087/2024 por una infracción del artículo 5.1.c) del RGPD**, por captar las mesas de todo un comedor con un sistema de video y de forma continua. Por su propia naturaleza, se trata de una ubicación en que los afectados por el tratamiento pueden permanecer largo tiempo, y en una situación en que puede verse afectado su derecho fundamental a la protección de datos de carácter personal, así como otros derechos y libertades, tales como su intimidad o el libre desarrollo de su personalidad, de manera especial, ya que suele acudirse a estos lugares en momentos de ocio. **Se establece una multa de 2.400 euros y medidas correctivas**.

En el **PS/00191/2023 contra VOX**, por la utilización de cámaras de videovigilancia que graban en exceso la vía pública y porque los carteles no contienen la información necesaria, se imputa también una infracción del 5.1.c) y otra del 13 del RGPD con una **multa de 500 euros cada una**. Como el local está cerrado, no se imponen medidas.

También se declara una infracción del artículo 13 del RGPD en el **PS/00096/2024 contra de Digiman Alicante, S.L.**, ya que el cartel informativo de la grabación no está visible al quedar oculto tras el cierre en horario nocturno. Se establece **sanción de 600 euros y medida correctiva** consistente en la colocación del cartel en zonas visibles.

El **PS/00420/2023** se inicia como consecuencia de una reclamación del arrendatario de una vivienda en la que indica que no ha sido informado de que, en el interior de esta, se encontraba instalada una cámara de videovigilancia, señalando asimismo que dicha cámara, por otro lado, no se encuentra debidamente señalizada mediante los preceptivos carteles informativos de zona videovigilada. Tramitado el procedimiento sancionador se

comprueba que son fotosensores de movimiento de la alarma que, cuando salta la misma, pueden captar imágenes y que hay carteles instalados relativos a la existencia de la alarma.

Dado que se ha acreditado la desconexión del sistema desde el momento de inicio del contrato de alquiler, así como la voluntad de la parte reclamada de no activarlo, no se realiza un tratamiento de datos, por lo que no se puede sancionar el hecho de no haber reflejado la existencia del sistema en el documento contractual inicial y se procede al **archivo del procedimiento**.

También terminaron en archivo las actuaciones de investigación **AI/00107/2024**, en un caso relacionado con el videoportero de una comunidad de propietarios. La resolución evalúa la proporcionalidad del tratamiento y concluye que el tratamiento es proporcional, ya que el videoportero no graba y solo se enciende si se pulsa el botón desde la placa de la calle, y a los 30 segundos se apaga y se desactiva. Se considera que **el tratamiento no excede de un uso personal o doméstico**. Es una muestra de que no todos los procedimientos terminan con sanción o declarando infracción.

También en el **PS/00337/2023 y el PS/00338/2023** iniciados como consecuencia de sendas reclamaciones recibidas a través del canal prioritario por la difusión de videos a través de redes sociales en el que se podía ver cómo iba perjudicando al reclamante la ingesta de alcohol. Los procedimientos **se archivan** al no existir certeza sobre la autoría de los hechos analizados: los sitios web donde se encontraban los vídeos han cerrado y se han facilitado varias direcciones IP asociadas a las cuentas desde donde se publicó y, además, ninguna de ellas se correspondía con el día en el que subió el vídeo.

En el caso del **E/06941/2018 contra Comisaria General de Información**, en virtud de lo indicado en sentencia dictada por el Tribunal Supremo en el marco de un recurso de casación, se retrotraen actuaciones y se dicta resolución de archivo. El caso se inició por la denuncia de 24 Magistrados destinados en órganos judiciales de Cataluña dirigida contra el Ministerio del Interior y el diario La Razón por la publicación, el día 3 de marzo de 2014, de una noticia titulada “La conspiración de los 33 jueces soberanistas” en relación con un manifiesto firmado por los denunciantes. En el artículo se indicaban sus nombres y apellidos, su destino como miembros de la judicatura y una fotografía de cada uno de ellos (33), que según manifestaron, no había sido facilitada por parte de los interesados.

Las actuaciones se retrotraen al momento de la realización de actuaciones previas de investigación, conforme a lo determinado en el artículo 122 del Reglamento aprobado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (vigente en el momento en que sucedieron los hechos objeto del expediente) y en el artículo 67 de la LOPDGDD. Tras la retroacción de actuaciones, se continúa el procedimiento, **finalizado en archivo** debido a la prescripción de las infracciones presuntamente cometidas.

También en archivo terminó el **PS/00424/2022 contra el Ayuntamiento de San Cristóbal De La Laguna**. Se inició con motivo de una reclamación, en la que se indica que la imagen de dos policías locales fue captada mediante fotografía o video con un terminal móvil particular por otros miembros del Cuerpo de Seguridad, cuando se encontraban de servicio en una operación, y fue cedida posteriormente a un periódico digital sin adoptar previamente ninguna medida no permitiera identificar a los policías. En el curso de la instrucción del procedimiento no ha quedado probado quién o quiénes proporcionaron al periódico digital la fotografía con la imagen de los agentes de la Policía Local publicada el 30/04/2021. Por tanto, **no se considera probada la infracción** del artículo 5.1.f) del RGPD.

Contra este mismo ayuntamiento se han tramitado dos expedientes sancionadores más, **PS/00064/2024 y PS/00131/2024** por no contestar a requerimientos de información durante unas actuaciones previas de investigación, declarando en ambos una infracción del artículo 58.1 del RGPD.

También contra un ayuntamiento es el **PS/00426/2022, en este caso el Ayuntamiento de Jerez de Los Caballeros**, por haber publicado en YouTube el discurso de una concejala en un pleno en el que comenta la existencia de una denuncia ante el Tribunal de Cuentas presentada por el reclamante, indicando su nombre y apellidos. Se declara la infracción de los artículos 5.1.f) y 32 del

RGPD y se ordena que en el **plazo de 2 meses el ayuntamiento acredite** haber adoptado medidas que garanticen la debida confidencialidad de los datos personales.

Contra el mismo ayuntamiento encontramos el **PS/00055/2024** por publicar, a pesar de las recomendaciones de su DPD, actas del Pleno del Ayuntamiento que incluían datos personales del reclamante (nombre, apellidos, NIF), un ciudadano que había formulado alegaciones a asuntos que se iban a debatir y aprobar en dichos plenos y había manifestado al Ayuntamiento su oposición a que sus datos fueran tratados en el acta. El Ayuntamiento estimó la oposición. Sin embargo, las medidas que adopta no son adecuadas. Por ello, **se imputan infracciones** de los artículos 5.1 c) y 32 del RGPD **y se imponen medidas correctivas**.

El **PS/00441/2022 contra el Ayuntamiento de Chinchón**, se inicia a partir de una reclamación por la publicación en su sitio web de los presupuestos para el año 2021, así como una relación en la que figuran todos los puestos de trabajo junto a la identidad de la persona que los ocupa. Se consideran incumplidos los artículos 5.1.f) del RGPD dado que no se ha garantizado la confidencialidad de los datos a través de medidas técnicas u organizativas apropiadas y el artículo 32 del RGPD dado que el Ayuntamiento no contaba con las medidas apropiadas, puesto que no tenía establecido ningún sistema de control de accesos. Además, se impone la adopción de las medidas adecuadas tendentes a que las publicaciones que realice en Ayuntamiento en su página web cumplan con la normativa aplicable en materia de protección de datos.

Por las mismas infracciones encontramos el **PS/00268/2023 contra Puerta De Leganés S.C. MAD** por la difusión de un contrato de uno de los socios de una cooperativa a otro socio a través de un correo electrónico. **Se imputan las infracciones** de los artículos 5.1.f) y 32 del RGPD (1.500 y 2.000 euros de sanción, respectivamente). **Como medida correctiva**, se ordena que acredite haber procedido a adoptar las medidas organizativas y técnicas adecuadas para garantizar un nivel de seguridad adecuado el riesgo y evitar que puedan remitirse datos personales sin base jurídica.

Muy similar es el **PS/00551/2022 contra la Universidad de Murcia** por haber facilitado a un tercero no legitimado documentación del reclamante relativa a un proceso de solicitud de una plaza de profesor, sin que ese tercero haya participado en dicho proceso. Se declaran las **infracciones de los artículos** 5.1.f) y 32 del RGPD.

Siguiendo en el ámbito de la Administración Pública, el **PS/00074/2024 contra el Ayuntamiento de Telde** se inicia por la implantación de un nuevo sistema de fichaje para el control de jornada en el que se utilizan 3 sistemas a la vez: biométrico (el reconocimiento facial era el sistema general de fichaje), app en el móvil por geolocalización, y conexión por web. **Se sanciona por tres infracciones administrativas**: por la infracción del artículo 35 del RGPD, por la infracción del artículo 9 del RGPD, y por la infracción del artículo 38 del RGPD y se establecen **medidas correctivas**.

En la misma línea se encuentra también el **PS/00545/2023 contra el Ayuntamiento de Fuentepelayo**, abierto como consecuencia de una reclamación de un trabajador por la implantación de un sistema de control horario mediante huella dactilar, sin comunicación ni información previa a los trabajadores ni a sus representantes, y sin evaluación de impacto. Además, paralelamente a este sistema de fichaje, los trabajadores rellenaban una "hoja de control horario". El sistema se suprimió por deficiencias en su funcionamiento por lo que no se incluyen medidas correctivas. Se imputan **infracciones de los artículos** 9, 35 y 13 del RGPD y, al ser una organización de las del artículo 77 de la LOPDGDD, se declaran las infracciones.

Y es que, durante el 2024, se han resuelto varios procedimientos sancionadores relacionados con el tratamiento de datos biométricos.

Como en los casos anteriores, es muy habitual que este tratamiento se realice con la finalidad de implantar sistemas de fichaje en el entorno laboral, como en el caso del **PS/00170/2023 contra CTC Externalización, S.L.** En este procedimiento se constatan tres infracciones: una infracción del artículo 13 del RGPD por la que se impone una **multa de 200.000 euros**, una infracción del artículo 32 del RGPD con una **multa de 65.000 euros** y, por último, una infracción del artículo 35 del RGPD por la que se impone una **multa de 100.000 euros**. Además de la multa,

se impone que, en el plazo de 6 meses, acredite haber procedido al **cumplimiento de medidas** para asegurar el cumplimiento con la normativa de protección de datos.

En relación con los datos biométricos podemos destacar, por el importe de la multa, el **PS/00484/2023 contra la Liga Nacional de Futbol Profesional (LNFP)**. Este procedimiento sancionador se abrió como consecuencia de la presentación de dos denuncias contra la LNFP por la instauración de un régimen de datos biométricos para acceso a los estadios en el sector de la grada de animación. La LNFP exige a los clubes la implantación de la medida, en función de unos fines (el acceso), a una parte del estadio (la grada de animación), con una base legitimadora (consentimiento), y ofertando a los clubes los medios a través de una sociedad de su grupo (SEFPSA, la misma que obligatoriamente por norma ha de aplicar los tornos de acceso).

Tras la tramitación de expediente sancionador se ha probado que LNFP es responsable del tratamiento de las operaciones de tratamiento consistentes en la contratación del sistema de reconocimiento biométrico, para procurar el control de acceso a los estadios de primera y segunda división en relación con la grada de animación, puesto a disposición de los clubes de fútbol y SAD. Los hechos probados ponen de manifiesto que es la LNFP quien ha decidido tratar datos biométricos para una determinada finalidad, implementar ese sistema y contratarlo, y ponerlo a disposición de los clubes de futbol y SAD, instándoles a su uso. Se estima que la LNFP es responsable del tratamiento, por lo que al configurar dichos datos como exigibles, debió haber efectuado una EIPD del artículo 35 del RGPD.

La multa por infracción del artículo 35 del RGPD, inicialmente prevista en 10.000.000 €, se ha rebajado a **1.000.000 euros** tras las alegaciones y documentación aportada por la LNFP a la propuesta de resolución. Se impone una **medida correctiva**: se estima procedente elevar a definitiva la suspensión temporal que evite la continuación del tratamiento de los datos personales a través del sistema de reconocimiento biométrico para los accesos a la grada de animación de los Clubes y SAD afiliados a la LIGA, en tanto no realice y supere una evaluación de impacto de protección de datos del tratamiento.

También relacionado con el acceso a recintos deportivos encontramos el **PS/00482/2023 contra el Club Atlético Osasuna**, que se inicia como consecuencia de una reclamación por la implantación de un sistema de Reconocimiento facial (RF) para acceder a su estadio. Antes de la implantación del sistema de reconocimiento facial, contaba con un sistema de acceso basado en la tarjeta de abonado o en su versión de tarjeta de abonado con código QR o tarjeta de abonado en el móvil, sistema que mantuvieron compatibilizándolo con el sistema de reconocimiento facial. Se examina si cumplen con el triple juicio de proporcionalidad. En la resolución se indica que se produce la infracción del artículo 5.1.c) del RGPD, ya que, se puede conseguir identificar al abonado que accede, pero no se acredita tal necesidad o por qué no se emplea un sistema de verificación, pero se omite la adecuación y pertinencia para la finalidad para la que se requiere. La EIPD no hace valoración alguna del problema que intenta abordar, porque no lo explica, solo ofrece este modo de acceso como voluntario y alternativo al que ya existe y al que se puede volver en cualquier momento. Se impone una **sanción de multa de 200.000 euros y se elevan las medidas provisionales a definitivas**.

El **PS/00432/2023 contra Loro Parque, S.A.** se inicia como consecuencia de tres reclamaciones. Los reclamantes, acuden a los parques Loro Parque y Siam Park, pertenecientes ambos al reclamado y reclaman porque al acceder se les ha recogido la huella dactilar, sin ser informados y sin saberlo porque no figura información alguna en las entradas cuando se adquieren. Se sanciona por el artículo 9.1 del RGPD con **multa administrativa de 250.000 euros**, dado que se recogen datos de todas las personas, de todas las edades. Además, **se imponen medidas correctivas**.

En el **PS/00419/2024 contra el Colegio Notarial de Aragón**, se trata de un sistema de fichaje para el control laboral con datos biométricos (huella dactilar). Se imputa una infracción del artículo 9 del RGPD por no contar con una circunstancia que levante la prohibición general del tratamiento de datos biométricos que establece el artículo 9.1 del RGPD y otra del artículo 35 también del RGPD por no superar una evaluación de impacto de datos personales. El importe de la **multa es de 10.000 euros**. A lo largo del procedimiento se analiza el tratamiento que realiza el Colegio llegando en a la

conclusión de que en este caso no actúa caso en el ejercicio de sus funciones públicas, a pesar de ser una Corporación de Derecho Público.

En el procedimiento **PS/00146/2023 contra Colegio Oficial de Ingenieros Técnicos Agrícolas y Peritos Agrícolas De Castilla Duero** por el envío por parte de su presidente al resto de colegios de la especialidad, de información y denuncias relacionadas con varios trabajadores del colegio y con un colegiado, tampoco se considera que ese acto pertenece a las funciones públicas que debe realizar el colegio, por lo que se imputa una infracción del 5.1.f) del RGPD con una **sanción de 10.000 euros**.

También en el ámbito laboral, el **PS/00414/2023 contra Societat Municipal D'aparcament** se inició como consecuencia de una denuncia por la que se ha tenido conocimiento de que se han producido grabaciones a los trabajadores ORA, en el ámbito laboral y sin su consentimiento, a través de una aplicación instalada en los dispositivos de trabajo (PDA) que usan habitualmente. Se imputa una infracción del artículo 5.1.a) del RGPD con una **multa administrativa de 40.000 €**.

En la misma categoría de asuntos laborales encontramos las actuaciones de investigación **AI/00034/2024** que terminaron con **archivo de una reclamación** por el uso por parte la jefa del reclamante de la cuenta de correo corporativa de éste para enviar tres correos electrónicos a clientes durante una jornada de huelga en la que no había ningún trabajador en el departamento del reclamante que pudiera hacerlo. La empresa avisa en la política de seguridad que tienen publicada en el portal del empleado de que se pueden utilizar las cuentas de correo corporativas por otras personas y de que las puede monitorizar y, además, se realiza un análisis de la ponderación para verificar si existe interés legítimo en este caso llegando a la conclusión de que sí.

Siguiendo con los procedimientos por el tratamiento de datos biométricos, el **PS/00361/2023 contra Cartonajes Bañeres, S.A.** se realiza por haber estado utilizando un sistema de reconocimiento facial para el fichaje laboral lo que dio lugar a la presentación de una reclamación en la que también se incluía la falta de respuesta de un ejercicio de acceso. Se imputan las siguientes infracciones con la imposición de las siguientes multas artículo 35 del RGPD, con **200.000 euros**; artículo 15 del RGPD, con **20.000 euros**. Además, se le da un plazo de 30 días para que acredite haber atendido al cumplimiento del ejercicio del derecho de acceso del reclamante.

También en relación con el derecho de acceso encontramos varios procedimientos.

El **PD/00132/2024 contra DIGI Spain Telecom, S.L.**, se abre como consecuencia de una reclamación en la que se manifiesta que, tras solicitar el acceso ante la parte reclamada del registro de llamadas entrantes y salientes mediante correo electrónico de fecha 24 de octubre de 2023, la entidad contestó facilitando solo el detalle del consumo. Se estima el acceso indicando que, del examen de la documentación aportada por las partes, ha quedado acreditado que la parte reclamante solicitó a la parte reclamada acceso al registro de llamadas entrantes y salientes de su teléfono móvil, y que ésta sólo le facilitó el registro de llamadas salientes. De acuerdo con lo expuesto, la denegación del acceso no puede basarse en una supuesta limitación del derecho de acceso impuesta por la Ley 25/2007, por cuanto esta ley no establece ninguna limitación para el ejercicio del derecho de acceso, en concreto y para el caso examinado, tampoco y expresamente respecto al listado de llamadas entrantes solicitado por la parte reclamante. Además, el derecho de acceso tiene que cohonestarse con la propia previsión del artículo 15.4 del RGPD, esto es, no debe afectar negativamente a los derechos y libertades de terceros.

En los procedimientos **PD/00116/2024 y PD/00129/2024 contra Ingeniería y Construcciones del Sur, S.A** se solicitó, además del derecho de acceso, la supresión de los datos personales del reclamante, que fueron incluidos por la parte reclamada en el portal LinkedIn, así como en la sección de noticias de su página web. La parte reclamada contesta, pero sin atender plenamente los derechos. Durante la tramitación de los procedimientos, ha procedido a dar respuesta a la solicitud de los reclamantes, atendiendo tanto al derecho de acceso, como el de supresión, suprimiendo los datos de LinkedIn y bloqueando los relativos a la relación laboral.

En el **PD/00143/2024 contra Samoygom Malacitana, S.L.** se estima una solicitud de acceso y limitación en la que pedía unas grabaciones de las cámaras de seguridad con ocasión de la caída de la interesada en un supermercado. Inicialmente no se remiten y después se contesta que ya no se pueden remitir porque han sido eliminadas. Se estima el procedimiento, constatándose que la parte reclamada ha infringido lo dispuesto en el Artículo 15 del RGPD y Artículo 18 del RGPD, aunque haya acreditado la contestación a la solicitud de reclamante 6 meses después.

En el **PD/00029/2024 contra Banco Bilbao Vizcaya Argentaria S.A.**, la parte reclamante ha solicitado el derecho de acceso a los datos personales que le conciernen. A lo largo del procedimiento, el reclamado ha atendido casi todas las peticiones de acceso hechas por el reclamante, salvo lo relativo a los datos de geolocalización. Por tanto, la reclamación se estima parcialmente ya que hay una parte de lo solicitado que el reclamado no acredita haberla enviado al reclamante.

El **PD/00248/2023 contra Universidad de León** por una solicitud de acceso respecto de los exámenes de la EBAU se abre por ausencia de respuesta. Durante la tramitación, la parte reclamada ha aportado documentación acreditando la comunicación remitida al interesado remitiéndole sus exámenes mediante la modalidad de copia en cumplimiento de una resolución del Comisionado de Transparencia de Castilla y León. El PD se estima con el argumento de que el derecho de acceso del artículo 15 RGPD engloba el suministro de toda la información prevista en el apartado primero de dicho artículo: deberá facilitarse al interesado no solo la documentación solicitada sino información como, entre otras, los fines del tratamiento del que estén siendo objeto sus datos, los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales o, de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.

También por un derecho de acceso, tenemos el **PD/00280/2023 contra Digiman Alicante, S.L.**, en el que se concluye que la parte reclamada sigue sin acreditar haber contestado el derecho de acceso ejercido por la parte reclamante. La parte reclamada está justificando que ha contestado el derecho de acceso, considerando que es suficiente la contestación al respecto suministrada por ellos a la AEPD como consecuencia de la tramitación de este procedimiento, en tanto en cuanto, la AEPD ha trasladado para alegaciones las presentadas por la parte reclamada a la parte reclamante. Sin embargo, dado que el responsable del tratamiento no acompaña copia de la necesaria comunicación que debe dirigir a la parte reclamante informándole sobre la decisión que haya adoptado a propósito de la solicitud de ejercicio de derechos, atendiendo éste o denegando motivadamente, procede estimar la reclamación.

Otro procedimiento relacionado con un derecho de acceso, en este caso procedente de otra autoridad de datos europea, es el **PS/00168/2023 contra Glovoapp23**. El procedimiento sancionador fue iniciado como consecuencia de una reclamación presentada ante la autoridad de protección de datos de Polonia por un trabajador de Glovo por la falta de atención de su derecho de acceso.

La principal alegación de Glovo se basa en que el reclamante no utilizó el canal establecido para el ejercicio de los derechos y que la falta de atención se debió a un error humano. Sin embargo, el reclamante utilizó el canal habilitado para la atención de los clientes, que es perfectamente válido para que los usuarios puedan ejercer sus derechos y Glovo no ha acreditado el error humano ya que se solicitó en tres ocasiones el acceso y en la tramitación de las peticiones intervinieron dos departamentos distintos de la empresa. Se sanciona a Glovo por infracción del artículo 15 del RGPD con **multa de 15.000 euros**.

También procedente de otra autoridad de control del EEE, en este caso la autoridad de protección de datos de Baja Sajonia (Alemania), se tramitó el procedimiento de apercibimiento **PA/00038/2023 contra Jcdecaux España, S.L.U.** En este procedimiento, se recibió reclamación en la que un participante reclamaba que presentó una solicitud de supresión de sus datos personales mediante correo electrónico y que no fue atendida en plazo. La entidad ha manifestado que no recibió dicho correo electrónico, pero que, tras recibir la comunicación por parte la AEPD, procedió a cancelar los datos del reclamante.

En el **PS/00154/2024 contra OK Mobility España, S.L.** procedente de Alemania, de la autoridad de Baden-Wurttemberg, se inició procedimiento sancionador transfronterizo por un derecho de acceso no atendido, en el que a través de las actuaciones de investigación realzadas se ha visto que no cumplen con el plazo de conservación de datos ni con el de información.

Se imputan las siguientes infracciones: del artículo 5.1.e) del RGPD con una **multa de 30.000€**; del artículo 13 del RGPD con una **multa de 18.000€** y del artículo 15 del RGPD con una multa de 12.000€. Además, también **se imponen medidas**, debiendo acreditar en el plazo de un mes que se proporcionó el acceso a los datos personales y en el plazo de tres meses que adecuaron los plazos de conservación al RGPD.

En cuanto a los procedimientos de cooperación europeos en los que ha participado la Agencia,

se puede destacar el dirigido contra **Tools For Humanity Corporation GMB**. La autoridad de protección de datos de Baviera ha adoptado una resolución que declara la infracción por parte de la empresa responsable del proyecto Worldcoin de varios artículos del RGPD y le insta a implantar las medidas correctivas oportunas. Esta resolución se produce una vez finalizado el procedimiento de cooperación entre autoridades competentes previsto en el artículo 60 del RGPD, en el que la AEPD ha cooperado de forma activa.

La finalización de este procedimiento sucede a la medida cautelar impuesta por la Agencia Española de Protección de Datos en marzo de 2024 en terreno nacional que, ante los indicios de graves incumplimientos, para evitar daños potencialmente irreparables y proteger los derechos de los ciudadanos, ordenó de forma inmediata el cese en la recogida y el tratamiento de datos personales que la compañía estaba llevando a cabo en España, así como el bloqueo de los que ya se habían recopilado.

La medida cautelar de la Agencia fue recurrida ante la Audiencia Nacional por parte de la empresa responsable de Worldcoin, que avaló la medida y rechazó el recurso al considerar que prevalecía "la salvaguarda del interés general que consiste en la protección del derecho a la protección de datos personales de los interesados frente al interés particular de la empresa".

La resolución de la autoridad de Baviera, donde la empresa tiene su establecimiento principal en Europa, ordena la **eliminación de todos los códigos de iris** almacenados desde el inicio del proyecto, almacenados sin las medidas de seguridad necesarias para el tratamiento de los datos biométricos; ordena que el tratamiento de iris futuro se realice sobre la base del consentimiento explícito del interesado, habiéndose utilizado una base jurídica incorrecta de tratamiento de datos biométricos especialmente protegidos de acuerdo con los artículos 6.1 y 9 del RGPD; y ordena que el tratamiento de códigos de iris futuro incluya el derecho a la supresión de los datos. Asimismo, en la resolución se constata que la empresa no implantó las medidas adecuadas para impedir el tratamiento de datos de menores, lo que será objeto de una investigación adicional posterior.

La resolución también prevé una serie de multas en caso de incumplimiento de las órdenes exigidas, sin perjuicio de las sanciones administrativas que correspondan por los incumplimientos ya declarados en materia de protección de datos personales, que serán objeto de una resolución sancionadora posterior de acuerdo con el Derecho administrativo alemán.

Otro procedimiento de cooperación relevante es el seguido contra **Meta Platforms Ireland Limited** en el marco del cual, se dictó una medida cautelar urgente de conformidad con el artículo 66.1 del RGPD contra Meta Platforms Ireland Limited para el cese de tratamiento en territorio español de datos personales en relación con las funcionalidades Election Day Information y Voter Information Unit, que se pretendía poner en funcionamiento desde el 30 de junio para el proceso electoral europeo.

La Agencia ordenó esta medida al considerar que el tratamiento de datos previsto por la compañía supone una actuación contraria al RGPD que, al menos, **incumpliría los principios de protección de datos de licitud, minimización de datos y limitación del plazo de conservación**.

La compañía Meta tiene su establecimiento principal en Europa radicado en Irlanda. Esta actuación de la Agencia se realizó en el marco del procedimiento establecido en el artículo 66.1 del RGPD que establece que, en circunstancias excepcionales, cuando una autoridad de control interesada –en este caso la AEPD– considere urgente intervenir para proteger los derechos y libertades de las personas, podrá adoptar medidas provisionales con efectos jurídicos en su territorio y con un periodo de validez que no podrá ser superior a tres meses.

En este contexto, la Agencia entiende que la adopción de medidas urgentes de prohibición temporal de estas funcionalidades estaba justificada para evitar la recopilación de datos, el perfilado de los usuarios y la cesión a terceros, impidiendo así que los datos personales puedan ser utilizados por responsables desconocidos y para finalidades no explícitas.

Volviendo al ámbito nacional, encontramos también diversos procedimientos por el uso ilícito de cookies.

Destaca el PS/00524/2023 contra **Techpump Solutions, S.L.**, en el que se realizaron actuaciones previas de investigación en todas las páginas web de la parte reclamada por la presunta vulneración de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). Se impone a la entidad, por la infracción del artículo 22.2 de la LSSI, **90.000 euros** debido a las deficiencias detectadas en la "Política de Cookies" de tres de sus páginas web.

También por infracción, del mismo artículo encontramos el **PS/00490/2023** en el que se impone una sanción a **NH Hotel Group** de **8.000 euros**. Al entrar en la página web del reclamado se instalan cookies de naturaleza técnica, de rendimiento, de funcionalidad, de Google Analytics y cookies propias y de terceros cuya finalidad no ha podido ser identificada, antes de que el usuario consienta. Además, si no se desea prestar el consentimiento se debe clicar "configuración", pero se siguen instalando las mismas cookies y lo mismo ocurre cuando se retira el consentimiento.

Similar es el **PS/00224/2023**. El procedimiento se inicia como consecuencia de una reclamación contra una página web propiedad del reclamado por el uso de cookies de medición de audiencias. Se sanciona con **2.000 euros** al responsable por infracción del artículo 22.2 de la LSSI porque la parte reclamada utilizaba Cookies de rendimiento, sin obtener consentimiento y sin facilitar información. Las citadas cookies de rendimiento y orientación son cookies analíticas de Google que podrían estar exentas, pero para ello, entre otras cuestiones, deben tener una finalidad estrictamente limitada a la medición exclusiva de la audiencia del sitio o de la aplicación y no se pueden reutilizar los datos para otras finalidades. También existe una infracción del artículo 13 del RGPD porque el acceso a la información de la política de protección de datos se encontraba inactivo, imposibilitando el acceso a la información con una **sanción de 2.000 euros**.

También relacionado con Google Analytics encontramos el **PA/00052/2023, contra la Fábrica Nacional de La Moneda y Timbre - Real Casa de la Moneda** porque el sitio web https://www.fnmt.es/ utiliza cookies analíticas de Google que transfieren datos a EE. UU.

Las Cláusulas Contractuales Tipo de Google se ajustan a las publicadas por la Comisión Europea en la Decisión 2010/87/UE. Sin embargo, el TJUE consideró que no eran válidas porque no impedían el acceso a los datos personales de los servicios de inteligencia estadounidenses. Por otro lado, Google adoptó medidas complementarias pero el CEPD consideró que no eran eficaces porque ninguna de ellas impide las posibilidades de acceso de dichos servicios de inteligencia.

Con fecha 10 de julio de 2023 se aprobó por la Comisión la Decisión de Ejecución (UE) 2023/1795 relativa a la adecuación del nivel de protección de los datos personales en el Marco de Privacidad de Datos UE-EE. UU, pero en la fecha en la que ocurrieron los hechos objeto de la reclamación, la transferencia internacional no podía ampararse en ninguna medida del Capítulo V del RGPD al haber declarado inválido el TJUE la anterior decisión de adecuación que amparaba las transferencias de datos personales a EEUU. La resolución declara la infracción del artículo 44 del RGPD.

Otro procedimiento de apercibimiento relacionado con las cookies es el **PA/00049/2023 contra Freepik Company S.L.**, que se inicia como consecuencia de una reclamación presentada por un ciudadano austriaco a través de NOYB por la utilización de cookies de Facebook en la página web de Freepik y su transferencia internacional.

Como consecuencia de todas las reclamaciones similares que se presentaron relacionadas con NOYB por la utilización de las aplicaciones de Facebook y Google para generar estadísticas y la posible transferencia internacional de datos al Gobierno de los EEUU, se creó un grupo de trabajo a nivel europeo en el que se decidió que se retirasen estas aplicaciones, pero que no se sancionara a los responsables de las páginas web (teniendo en cuenta que las reclamaciones se presentaron justo después de que se hiciera pública la sentencia Schrem II).

Se dirige un apercibimiento al responsable por la infracción del artículo 44 del RGPD, **sin que sea necesario poner medidas correctivas** al haber eliminado el reclamado el login federado de Facebook.

Otro procedimiento de apercibimiento destacado es el **PA/00019/2023 contra el Instituto para la Diversificación y Ahorro de la Energía (IDAE)**. Se presenta reclamación porque para optar al cobro de una subvención, el beneficiario se encontraba obligado a colocar un cartel informativo en la puerta de su casa durante un período de 5 años. En el citado cartel se deben incluir los datos del beneficiario, el presupuesto del proyecto y la cantidad de la subvención recibida por parte del organismo público. La parte reclamante considera que la citada obligación vulnera la normativa de protección de datos ya que, a través de esta, se le impone la revelación de sus datos identificativos y los de la obra quedando expuestos a todos los viandantes, los cuales no tienen por qué tener acceso a los mismos.

Las actuaciones realizadas han permitido comprobar que, tratándose de subvenciones recibidas por personas físicas, ninguna norma establece la obligación impuesta por IDAE sobre la inclusión de los datos personales de los beneficiarios en los carteles que publicitan la financiación. Se considera vulnerado el artículo 32 del RGPD por la falta de medidas técnicas y organizativas adecuadas al riesgo al posibilitar la exhibición de datos de carácter personal de personas físicas beneficiarias de ayuda. **Se impone como medida** que la entidad responsable adecúe su actuación a la normativa de protección de datos personales.

También por infracción del artículo 32 del RGPD encontramos el **PS/00447/2023 contra Dimagaza, S.L.**, iniciado como consecuencia de una reclamación en la que se indica que la empresa publica un acta de acuerdo de despido colectivo en el tablón de anuncios de la empresa, conteniendo un listado de 43 trabajadores despedidos con sus datos personales sin anonimizar. **Se impone multa de 15.000 euros**.

En cuanto al importe de las multas impuestas, el sector del suministro de agua y energía es el que concentra un importe mayor en 2024.

El procedimiento con la multa más elevada en 2024 es el **PS/00216/2023 contra Energya VM Gestión De Energía S.L. (en adelante Enérgya-VM)**, relacionado con una investigación policial sobre los encargados de dicha empresa. Las actuaciones policiales detectaron que una de las encargadas del tratamiento (Nivalco) de la comercializadora Enérgya-VM, tras tener acceso a la base de datos de Naturgy Iberia, S.A. procedió a la captación fraudulenta de clientes para Enérgya-VM. Las contrataciones se realizaban mediante engaño haciendo creer a los interesados que el contacto telefónico se realizaba por cuenta de su compañía. A principios de septiembre de 2019, Naturgy Iberia, S.A. alertó a Enérgya-VM de las actuaciones de Nivalco y Enérgya-VM procedió a realizar una auditoría y a establecer el sistema de doble verificación del consentimiento. Aunque Enérgya-VM tomó algunas medidas, las contrataciones engañosas continuaron y no rescindió el contrato con Nivalco hasta el 30 de junio de 2020. Se **sanciona a Enérgya-VM** por las siguientes infracciones:

- Infracción del artículo 5.1 a) del RGPD por falta de lealtad y transparencia. **Multa de 2.500.000 euros**.
- Infracción del artículo 5.2 del RGPD. **Multa de 2.500.000 euros**.

También destaca, por el elevado importe de la multa impuesta, el procedimiento **PS/00145/2023 contra I-DE Redes Eléctricas Inteligentes, S.A.U.** En este caso, el procedimiento sancionador se inicia por la brecha de datos personales sufrida en un aplicativo web de la empresa distribuidora de electricidad, perteneciente al Grupo Iberdrola. La brecha fue provocada por un ataque informático aprovechando una vulnerabilidad del aplicativo web de I-DE y afectó a la confidencialidad de 1,35 millones de clientes.

Se impone una **multa de 2.500.000 euros** por la infracción del 5.1.f) del RGPD y otra de **1.000.000** por infracción 32 también del RGPD.

La brecha también afectó a casi 2 millones de clientes de otras dos empresas del Grupo, pues el atacante consiguió vulnerar la separación lógica existente en la base de datos común de las entidades del Grupo Iberdrola. Esta base de datos se encuentra a cargo de Iberdrola SA en su condición de encargado del tratamiento.

Por esta razón, contra **Iberdrola SA**, se inició el **PS/00221/2023**. En este caso se sanciona al encargado en lugar de a los responsables porque Iberdrola presta servicios de encargado a las compañías del grupo y no realizó un análisis de riesgos sobre los riesgos inherentes del tratamiento que él realiza consistente en almacenar los datos personales de diferentes responsables del tratamiento en una misma base de datos, ni adoptó medidas adecuadas, pues la separación lógica existente en la base de datos permitía acceder a datos personales de clientes de otras empresas. Se impone **una multa de 2.000.000 euros** por la infracción del 5.1.f) del RGPD y otra de **1.000.000** por infracción 32 del RGPD.

También por infracciones de los artículos 5.1.f) y 32 del RGPD, entre otras, en el sector de los seguros,

y con una **multa total de 4.000.000 de euros** encontramos el **PS/00453/2023 contra Generali España, Sociedad Anónima de Seguros y Reaseguros** iniciado como consecuencia de varias reclamaciones en las que se indica que se ha producido una brecha de datos personales. A raíz de la investigación realizada se conoció que un ciberdelincuente forzó las credenciales de un corredor y tuvo acceso a numerosos datos personales tratados por la aseguradora Generali, incluidos de exclientes de la entidad. Durante la investigación se ha comprobado que no tenía medidas de seguridad suficientes que hubieran permitido que el impacto de la brecha de datos personales fuese menor, que carecían de medidas de seguridad básicas, que tenían los datos de clientes y exclientes en una misma base de datos y que carecían de evaluación de impacto. Por ello se le imputan las siguientes infracciones:

- Artículo 5.1.f) del RGPD, vinculada a la falta de medidas, de cualquier tipo, y se ha materializado en que los datos se han expuesto datos en Internet. **Multa de 800.000€.**
- Artículo 32 del RGPD está relacionada con la falta de medidas de seguridad básicas. **Multa de 800.000€.**
- Artículo 25 del RGPD está asociada a un mal diseño desde el principio en el que los datos de clientes y exclientes se incluían en la misma tabla. **Multa de 1.600.000€.**
- Artículo 35 del RGPD por la falta de la realización de una evaluación de impacto. **Multa de 800.000€.**

Además, se da un plazo de 3 meses para que hagan una evaluación de impacto.

Por infracciones de los artículos 5.1.f) y 32 del RGPD, en este caso en el sector financiero, encontramos

el **PS/00477/2023 contra Caixabank, S.A.** Este procedimiento sancionador se inicia como consecuencia de la reclamación en la que se expone que, al intentar uno de los reclamantes realizar cualquier operativa con sus cuentas a través de la banca online, se precisa de la firma de la persona autorizada incluso en otra cuenta compartida con otro de los reclamantes, con el que la persona autorizada no tiene ningún tipo de relación.

Asimismo, dicho tercero, al acceder al área personal a través de la aplicación del banco, puede visualizar no solo la información relativa a las cuentas y a los productos vinculados a las mismas en las que figura como autorizado, sino que también visualiza la información relativa a

las tarjetas vinculadas a la tercera cuenta ajena a dicho tercero. A raíz de lo ocurrido, presentan numerosas reclamaciones ante la parte reclamada, así como una reclamación ante el Banco de España, sin que se haya solucionado la incidencia, llegando hasta la AEPD. Se imputa infracción del artículo 5.1.f) del RGPD con una **multa de 500.000€**. El artículo 25 del RGPD se imputa por inadecuación del diseño de la aplicación informática de la entidad financiera con una **multa de 3.000.000€**.

Por las mismas infracciones de los artículos 5.1.f) y 32 del RGPD, en el mismo sector y con **multas de 120.000€ y 240.000€**, respectivamente, encontramos el **PS/00424/2023 contra 4Finance Spain Financial Services S.A.U.** Este procedimiento también se inició por una brecha de datos personales de 4Finance Spain Financial Services notificada a la Agencia fuera de plazo. La entidad no comunicó la brecha a los clientes hasta que recibió una orden de la Agencia. Además, también se han recibido varias reclamaciones. Como consecuencia de la brecha, los atacantes accedieron a las cuentas personales de miles de clientes y solicitaron créditos personales (en aquellos casos donde previamente se había ya concedido uno previamente); posteriormente se ponían en contacto con la víctima y simulaban ser la entidad crediticia y les pedían la devolución del prestamos que, según ellos, había sido concedida por error. **Hay 426 clientes afectados**. A través de la investigación realizada se ha comprobado que no existían medidas de seguridad adecuadas.

También en el sector financiero, encontramos el **PS/00255/2023 contra el Banco Santander**. Se inició por una reclamación por facilitar datos bancarios a terceros. En este caso se declaran dos infracciones: 5.1.f) y 32.1 del RGPD con **multas de 50.000 y 20.000 €** respectivamente. Además, se da un plazo de seis meses para que el banco adopte las medidas adecuadas.

En el mismo sector destaca el **PS/00677/2022 contra Banco Bilbao Vizcaya Argentaria, S.A.** por la comisión de las siguientes infracciones: artículo 6.1 del RGPD en relación con la contratación no autorizada de productos y con la incorporación de datos personales en los sistemas de información crediticia, artículo 25 del RGPD y artículo 32 del RGPD por la falta de medidas de seguridad en relación con los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales con los procedimientos de contratación de productos financieros. Con una **sanción total de un millón de euros**.

También por contratación fraudulenta, con infracción del artículo 6.1 del RGPD encontramos el **PS/00236/2024 contra Mapfre Inversión Sociedad de Valores S.A.** por contratar seis fondos de inversión sin la autorización de los reclamantes. Mapfre actúa por medio de un agente y en una parte de su respuesta, indica que el agente introdujo su móvil en el aplicativo de la entidad para recibir el PIN que le permitió tratar las órdenes de inversión, para que después fueran ratificadas por los clientes. El reclamante indica que debe ser él quien autorice mediante esa firma electrónica con su móvil, o bien de forma manuscrita; que el agente nunca ha sido autorizado para recibir esas claves y firmar una orden de venta o suscripción. Se imputa infracción del artículo 6.1 del RGPD con **300.000 euros de multa**.

Por la misma infracción encontramos el **PS/00392/2023 contra Partido Popular**, iniciado como consecuencia de una reclamación por la difusión en el programa electoral del PP de una fotografía con una imagen de la reclamante, sin su consentimiento. Se sanciona con una **multa de 5.000 euros** pues han utilizado la imagen de la reclamante para un fin distinto sin base de legitimación.

Otro de los grupos de actividad mayoritario en los procedimientos de la Agencia es el de los servicios de Internet, con un 19% de los procedimientos.

En este ámbito podemos destacar el **PS/00652/2022 contra Display Connectors, S.L.** por la publicación en distintos medios de comunicación de una noticia ilustrada con un vídeo en el que aparecen imágenes de una pantalla de ordenador en la que se visualiza una hoja de Excel con los datos personales de mujeres registradas en el sistema como víctimas de violencia de género, y distintas clasificaciones en función de sus circunstancias concretas. Se imputa infracción del artículo 5.1.c) del RGPD y **multa de 187.000 euros**.

La misma infracción se imputa en el **PS/00335/2023 contra El León de El Español Publicaciones**, por haber publicado un vídeo de una persona perjudicada por la ingesta del alcohol sin anonimizar. El vídeo fue retirado atendiendo el requerimiento de la Agencia y se imputa una infracción del artículo 5.1.c) del RGPD con una **multa de 10.000 euros**.

Similar es el **PS/00125/2024 contra Eda TV Consulting, S.L** y el **PS/00126/2024 contra una persona física** por la publicación de imágenes en Telegram. En los procedimientos se pondera el derecho a la libertad de expresión y el de la protección de datos. En ambos se imputa una infracción del artículo 5.1.c) del RGPD y se les impone una **multa de 5.000 euros**.

También se analiza la libertad de información versus protección de datos en el **PS/00365/2022**. La reclamación es por la aparición en el canal de YouTube de la parte reclamada, de la videoconferencia de un acto procesal de derecho civil, en la que el reclamante, en nombre de varios clientes, denuncia contra el honor contra el reclamado, entre otros. En el vídeo se ve al reclamante (aunque con mascarilla y de lejos,) y se oye su voz. En la parte inferior del vídeo de YouTube, figura además una nota del reclamado en el proceso, donde se puede ver el nombre y apellido del reclamante con un enlace que lleva al dominio del reclamado y la referencia al auto que resuelve el asunto. Se imponen **diversas medidas**:

- Retirada o distorsión de la voz del reclamante y de las notas a pie de video que le identifiquen,
- Retirada o anonimización de los enlaces que albergan la citada nota de prueba en la web del reclamado que permiten identificar al reclamante con su nombre y apellidos
- Retirada o modificación de los documentos creados enlazados por el reclamado que hacen posible el acceso al contenido del acuerdo de inicio y de la propuesta de resolución de este procedimiento, de tal modo que imposibilite su acceso y puesta en conocimiento de los datos que identifican al reclamante o le hacen identificable por terceros.

Esta **resolución fue recurrida**, y tras el recurso de reposición RR/00116/2024 se rebaja la cuantía de la multa, de **10.000 euros en 5.000 euros** por infracción del artículo 5.1.b) del RGPD.

Por publicaciones en Internet encontramos el **PS/00177/2023**, en el que el reclamado publica en sus redes sociales una serie de documentos, entre ellos también partes médicos, que contienen datos personales de la parte reclamante, a fin de justificar su denuncia por racismo contra la misma. Además de datos médicos se publican nombre y apellidos, imagen de la reclamante, DNI de la reclamante, dirección… Ha quedado constatado que la parte reclamada publicó en su perfil de la red social Facebook documentos que contienen datos personales identificativos y de salud de la parte reclamante sin respetar lo establecido en los artículos 9 y 6.1 del RGPD. Por ello se imputan infracciones: artículos 9 y 6 RGPD. Con **sanciones de 5.000€ en ambos casos y se impone la medida de la retirada de la publicación**.

En el **PS/00202/2023 contra Play Ful Kids, S.L.**, después de que algunos clientes insertaran reseñas negativas en el perfil de Google de la reclamada, la administradora de la empresa les contactó por WhatsApp remitiendo un vídeo y advirtiendo que lo haría público si no retiraban las reseñas. Además, el video fue publicado en el perfil de Twitter del ayuntamiento. Se sanciona con **multa de 3.000 euros** por infracción del artículo 6 del RGPD.

También por publicaciones en redes sociales, encontramos el **PS/00434/2023 contra Autocines 2015, S.L**, que se inició como consecuencia de una reclamación en la que exponían que Autocines 2015 subió a su perfil de las redes sociales Facebook e Instagram una fotografía de su hijo de 6 años, tomada mientras estaba en sus instalaciones jugando, sin solicitar el permiso de los progenitores, siendo utilizada posteriormente para ilustrar publirreportajes en dos diarios nacionales, en los que aparecía como foto principal. La entidad reconoce haber publicado la imagen sin consentimiento paternal. Se comprueba que la imagen ya no aparece en las RRSS de la entidad reclamada, ni en los periódicos. Se imputa una infracción del artículo 6 del RGPD y se impone una **multa de 5.000 euros**.

También por infracción del artículo 6 del RGPD encontramos el **PS/00275/2023 contra Kenai Media** consecuencia de una reclamación en la que se indica que ha publicado una película con la imagen de la reclamante sin su autorización. Se sanciona con una **multa de 10.000 euros**.

En el **ámbito sanitario** encontramos varios procedimientos reseñables.

Entre ellos el **PS/00351/2023 contra HM Hospitales 1989 S.A.**, que se abrió tras la realización de una investigación abierta como consecuencia de denuncia. El denunciante expone distintas deficiencias de seguridad relacionadas con el mantenimiento de un servicio de software desarrollado por la misma y utilizado por todos los centros hospitalarios de la mercantil denunciada. Como consecuencia de la denuncia, la directora de la Agencia acordó abrir una investigación de oficio donde quedaron puestos de manifiesto posibles incumplimientos en materia de datos personales. Se impone a HM Hospitales 1989 por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una **multa de 200.000 euros**. **No hay medidas correctivas** porque a lo largo del procedimiento han realizado actuaciones para cumplir con el RGPD.

El **PS/00063/2024 se inició contra Boston Scientific Ibérica** por una brecha de datos personales que notificó a la Agencia. En la notificación reconocían que había existido algún acceso por parte de una persona de Alemania y de personal del Hospital, sin llegar a concretar. No consideraron necesario notificar a los más de 26.000 afectados; no obstante, desde la Agencia se les ordenó que lo hicieran. Durante la investigación, se ha comprobado que no tenían medidas de seguridad suficientes. Se imputan las siguientes infracciones: 5.1.f) del RGPD con **multa de 75.000€**; 32 del RGPD con **multa de 250.000€** y 34 del RGPD con una **multa de 100.000€**.

El PS/00317/2022 contra Centro médico Salus Baleares, S.L, se inició por una reclamación de un paciente que acudió a una clínica donde tomaban la temperatura en un dispositivo electrónico situado en una pared, pudiendo las personas que estaban en la sala de espera y en la recepción visualizar la temperatura que tomaban a otros pacientes. El reclamante aportó varias fotografías de varios momentos donde se podía observar que la temperatura seguía estando en la pantalla del dispositivo durante unos segundos a pesar de que el paciente ya se hubiera retirado del equipo. Se imputan dos infracciones del RGPD: articulo 5.1.f) con una **multa de 20.000€** y artículo 32 con una **multa de 10.000€**.

También relacionado con datos de salud encontramos el **PS/00541/2022 contra GSMA Limited porque para la celebración del Mobile World Congress (MWC 2022)** solicitó a los empleados de los proveedores de la Fira de Barcelona que registraran en una plataforma su certificado COVID, certificado de recuperación de COVID 19 o prueba PCR negativa.

La reclamada señala como base de legitimación para el tratamiento de los datos de salud de los empleados de los proveedores las contempladas en el artículo 6.1. del RGPD, letras c) y d), y considera que concurren las circunstancias recogidas en el artículo 9.2 del RGPD, letra g), existencia de un interés público esencial y h) prevención de la salud de los trabajadores. Se analiza la normativa autonómica vigente en aquel momento, que resultaría aplicable al evento, y en la misma no se establece el tratamiento de los datos de salud. Por ello el tratamiento efectuado no puede basarse en el artículo 6.1.c) del RGPD n en la circunstancia del artículo 9.2.g). Tampoco puede basarse en la protección de un interés vital, por cuanto no se justifica la necesidad del tratamiento por tratarse de empleados de otras entidades y existir medidas menos invasivas como proporcionar equipos de protección. No concurre tampoco la circunstancia de la letra h) del artículo 9.2 del RGPD pues la reclamada no puede ampararse en que realizaba las labores de coordinación previstas en el artículo 24 de la Ley de Prevención de Riesgos Laborales, pues no existen indicios de que la documentación COVID se solicitara en coordinación con los proveedores, empresarios de los empleados de montaje.

Además, según el artículo 22 de la Ley, la vigilancia de la salud requiere el consentimiento de los empleados, salvo excepciones tasadas que no pueden aplicarse de modo general a todos los trabajadores, sobre todo cuando podían haberse adoptado medidas que suponían menor injerencia en los derechos de los trabajadores. En cuanto a la infracción del artículo 14 del RGPD, la reclamada indica que la información sobre el tratamiento de los datos la facilitaba el proveedor a sus trabajadores. Sin embargo, la obligación de informar recae en el responsable del tratamiento que no puede desplazar su cumplimiento a terceros. La política de privacidad existente en la web de la reclamada no alude a los datos de los empleados de los proveedores y no contiene todas las previsiones que exige el RGPD.

Se sanciona a GSMA Limited por lo siguiente:

- Infracción del artículo 9 del RGPD con una **multa 300.000 euros**.
- Infracción del artículo 6del RGPD con una **multa de 200.000 euros**.
- Infracción del artículo 14 del RGPD con una **multa de 100.000 euros**.

Otro procedimiento en el que se tratan datos de salud, también relacionados con COVID-19, es el **PS/00363/2023**, iniciado como consecuencia de la presentación de una reclamación contra una persona física, organizadora de la carrera X Gomera Trail en septiembre de 2021, por pedir certificado COVID, de recuperación, o test 48 horas antes de disputarse. No se acreditó que se hubiera informado del tratamiento de dichos datos, conforme señala el artículo 13 del RGPD y tampoco aportó, a pesar de serle requerido, el RAT, registro actividades del tratamiento. Se imponen las **siguientes sanciones**: por infracción del artículo 9 del RGPD, **8.000 euros**; por infracción del artículo 13 del RGPD, **6.000 euros** y por infracción del artículo 30 del RGPD, **1.000 euros**.

El **PS/00078/2024 contra Dentalcuadros** se sigue con motivo de una notificación de brecha de disponibilidad de datos personales. Los hackers cifraron los datos para pedir posteriormente un rescate. Se vieron comprometidos los datos identificativos y de salud dental de los pacientes de la clínica. Se imputan infracciones del artículo 32 y del artículo 33 del RGPD con **multas de 6.000 euros en ambos casos**.

Similar es el caso del **PS/00648/2022 contra Electrónica Informática Instrumentación y Telecomunicaciones S.A.** iniciado también por una brecha de datos personales, de disponibilidad por cuanto el ataque se materializó con el cifrado de discos y el borrado de máquinas virtuales, quedando acreditado que se recibió un mensaje por parte del grupo criminal Ransomware (Hive) confirmando la autoría del ataque y solicitando pago del rescate. Se sanciona por las siguientes infracciones y con las siguientes multas:

- Infracción del artículo 5.1.f) del RGPD, multa administrativa de cuantía **50.000 euros**.
- Infracción del artículo 32 del RGPD, multa administrativa de cuantía **20.00 euros**.
- Infracción del artículo 28 del RGPD, multa administrativa de cuantía **20.000 euros**.
- Infracción del artículo 30 del RGPD, multa administrativa de cuantía **20.000 euros**.

Se imponen además medidas correctivas.

En el sector de las telecomunicaciones también se han llevado a cabo varios procedimientos sancionadores relevantes.

Como el **PS/00291/2023 contra Telefónica de España SAU**, abierto como consecuencia de la notificación de una brecha de confidencialidad de datos personales en la que los datos afectados fueron los números de teléfonos fijos y los datos del equipamiento. Ha afectado a más de 1,4 millones de clientes. La brecha se produjo como consecuencia de un acceso masivo (de 55.000 solicitudes al día a 4 millones de solicitudes y por un único usuario), a través de un portal web (que era a través del cual accedían los empleados), a datos de clientes. Se sanciona a Telefónica por una infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD, c**on multas de 500.000 y 800.000 euros**.

El **PS/00332/2023 contra Orange Espagne, S.A.U.** se inició con motivo de una reclamación por el duplicado de la tarjeta SIM de la reclamante. Se sanciona a Orange por las siguientes infracciones:

- Infracción del artículo 6 del RGPD: **200.000 euros de multa**, por la emisión de un duplicado de tarjeta SIM que no había solicitado la reclamante;
- infracción del artículo 25 del RGPD: **un millón de euros de multa** por no haber adoptado desde el diseño del procedimiento medidas adecuadas para evitar errores.

También se impone a Orange la **medida** consistente en que en el plazo de 6 meses notifique a esta Agencia las medidas que ha adoptado para garantizar que la solicitud de duplicado se presenta por el titular del número de teléfono, sea cual sea el procedimiento utilizado para su emisión.

En el **PS/00364/2023 contra Vodafone España, S.A.U.** la parte reclamante manifiesta que recibió una factura del servicio de línea móvil de la reclamada, y que en la misma constaban los datos identificativos de un tercero ajeno a la reclamante. Se imputa el artículo 5.1.d) del RGPD con una **multa de 112.000 euros**.

También contra **Vodafone España, S.A.U. encontramos el PS/00306/2023**, en este caso por no atender adecuadamente un requerimiento en el marco de unas actuaciones de investigación. Se le requirió para que confirmase si una determinada llamada se había producido entre dos números, suministrando los dos números, la fecha y la hora, tal y como indica el artículo 52.3 de la LOPDGDD. Era una mera confirmación, no se le requería dato alguno sobre el llamante. El requerimiento se ajusta a las previsiones del artículo 52.3 de la LOPDGDD y no se le solicita ningún dato de tráfico, ningún dato sobre la llamada entrante. Se imputa una infracción del artículo 58.1 del RGPD, con imposición de **multa de 200.000**, junto con la **medida correctiva** consistente en facilitar la información requerida.

También por no atender adecuadamente solicitud de información es el **PS/00339/2023 contra Telefónica de España, S.A.U.** se imputa una infracción del artículo 58.1 del RGPD, con imposición de multa de **90.000 euros**.

Relacionados con menores encontramos varios procedimientos

Como el **PS/00557/2023 contra Associacio Oasis Cultural** iniciado de oficio a raíz del conocimiento de un video difundido en TikTok en el que se veían a varios jóvenes realizando bailes con connotaciones sexuales. El vídeo se grabó en una discoteca de Barcelona y en la difusión que se hizo se incluía el nombre del perfil de la discoteca. En el marco de las actuaciones de investigación se realizaron diversas solicitudes de información sin respuesta. Se imputa una infracción del artículo 6.1 con una **multa de 10.000 euros**.

También relacionadas con datos de menores, encontramos varias retiradas de contenido urgentes de Instagram: **AI/00093/2024, AI/00041/2024, AI/00134/2024 y AI/00144/2024,** entre otras.

Siguiendo con el tratamiento de datos de menores de edad, el **PS/00072/2024 contra el Ayuntamiento de Alguazas** se abrió tras denuncia a raíz de la convocatoria de unas olimpiadas para personas menores de edad, con varias infracciones del RGPD:

- Tres infracciones del artículo 6.1 del RGPD: por la inscripción de datos de menores en el grupo de WhatsApp creado por el Ayuntamiento, por el tratamiento de datos personales de menores de 14 años en el formulario de inscripción y por la publicación de imágenes de los jóvenes en la web del Ayuntamiento, todo ello sin haber acreditado que dicho tratamiento de datos pueda basarse en una de las causas de licitud contempladas en el citado artículo 6.1 del RGPD.
- Artículo 7 del RGPD: porque el formulario de inscripción no ofrecía la posibilidad de marcar o desmarcar la opción de recibir comunicaciones.
- Artículo 13 del RGPD: por la falta de información.
- Artículo 37 del RGPD: por la falta de DPD.

A lo largo del procedimiento se han corregido las infracciones por lo que **no se proponen medidas**. Al ser una organización de las incluidas en el artículo 77 de la LOPDGDD se declara la infracción.

El **PS/00471/2023** se inició como consecuencia de una comunicación de la policía en la que pone de manifiesto una denuncia de los padres de una menor de 13 años a la que un tiktoker, sin el consentimiento de sus padres, ha grabado una entrevista sobre su vida sexual y la ha difundido a través de las redes sociales. Se imputan las siguientes infracciones: artículo 9.1 del RGPD por tratar datos de la vida sexual con **multa de 3.000 €**; artículo 6.1 del RGPD por haber grabado a una menor sin el consentimiento de sus padres con una **multa de 3.000€**; artículo 5.1.c) del RGPD por difundir datos excesivos en las redes sociales con **multa de 3.000€** y artículo 13 del RGPD por no dar información adecuada con **multa de 1.000€**.

También por una infracción del artículo 5.1.c) del RGPD encontramos el **PS/00151/2023 contra Azulejos Peña**. En este procedimiento, el reclamado solo da como opción la transferencia para reembolsar el precio en una devolución y se

considera que el tratamiento del dato del IBAN no resulta en ningún caso "necesario" para la finalidad para la que se recoge. Se sanciona a la reclamada por Infracción artículo 5.1.c) del RGPD con una multa administrativa, **70.000 euros** y se establecen **medidas correctivas**.

Se declara igualmente una infracción del Artículo 5.1.c) del RGPD, entre otras en el **PS/00070/2023 contra la Consejería de Economía, Conocimiento y Empleo**. El reclamante manifiesta que, al presentar un escrito dirigido a la Consejería de Economía, Conocimiento y Empleo del Gobierno de Canarias, a través de su página web, se le solicita como obligatorio que indique si es "hombre/mujer/no binario" y que afecta a su intimidad y a su orientación sexual. Se considera que el término "no binario" es excesivo para lograr la finalidad pretendida estadística. Se declara también una infracción del artículo 9.1 del RGPD: tratamiento de categorías especiales de datos personales ("no binario" es identidad sexual o identidad de género, esto es, el sexo sentido y no el asignado al nacer). No concurre para el caso concreto excepción del artículo 9.2 del RGPD que levante la prohibición. Se imponen, además, **medidas correctivas**.

Por una denuncia se inició el **PS/00324/2023 contra el Ministerio para la Transición Ecológica y el Reto Demográfico**. Tras la denuncia se abrieron actuaciones previas de investigación, para analizar el Sistema BOSCO, aplicación utilizada por el Ministerio para la Transición Ecológica y el Reto Demográfico para la reducción de la factura eléctrica a las personas en situación de vulnerabilidad. En la resolución administrativa se constata que se han producido las infracciones de los artículos 13, 22 y 25 del RGPD, declarando la comisión de dichas infracciones. También se imponen medidas correctivas, pero no se paraliza el tratamiento.

También tras una denuncia se inició el **PS/00382/2023 contra la secretaría de Estado de Seguridad, Dirección General de Coordinación y Estudios, del Ministerio del Interior** por posible vulneración de la normativa de protección de datos del Sistema de Seguimiento Integral de los casos de Violencia de Género (Sistema VioGén) del Ministerio del Interior. Dicho sistema consiste en una aplicación web diseñada para coordinar las actuaciones de los profesionales públicos españoles que se encargan del seguimiento, asistencia y protección de las mujeres denunciantes de violencia de género y de sus hijos.

Se dicta resolución de declaración de la infracción de los siguientes artículos: infracción del artículo 20 de la LO 7/2021; infracción del artículo 35 de la LO 7/2021; infracción del artículo 41 de la LO 7/2021. Se imponen también **medidas correctivas**.

Relacionado con los datos del sistema VioGén encontramos el **PS/00279/2023 contra la Comandancia de Toledo de la Guardia Civil**, iniciado como consecuencia de dos denuncias presentadas por dos asociaciones de guardias civiles y de la información publicada en la Revista Digital de Suboficiales de la Guardia Civil, en la que se ponía en conocimiento de la AEPD la existencia en la Comandancia de la Guardia Civil de Toledo de una base de datos personales al margen de las declaradas por la Dirección General de la Guardia Civil. En la misma figuraban datos de víctimas de violencia de género y agresores y de guardias civiles. Se declaran las siguientes infracciones: del artículo 11.1, del artículo 28 y del artículo 37 de la LO 7/2021.

El **detalle de las resoluciones de todos los procedimientos** indicados puede encontrarse en la página web de la Agencia **www.aepd.es**, en el apartado de **Publicaciones y Resoluciones**,

o introduciendo en el buscador el código indicado para cada uno de los casos descritos. Las resoluciones se publican en cumplimiento del mandato de publicidad que dispone el artículo 50 de la LOPDGDD.

6. Una organización resiliente y en permanente mejora

6.1 Captación de talento y compromiso con el bienestar laboral

La Agencia Española de Protección de Datos cuenta con una Secretaría General, a la que corresponde la prestación de los servicios comunes de la entidad, bajo la inmediata dirección de la Directora de la AEPD.

En 2024, la Relación de Puestos de Trabajo (RPT) de la AEPD fue objeto de varias ampliaciones para permitir la incorporación de las personas que habiendo superado procesos selectivos habían obtenido puesto en la AEPD (1 CGSIAE, 4 GACE y 2 TAI).

Durante 2024 se convocaron y resolvieron cuatro convocatorias de libre designación para cubrir un total de 23 puestos, así como dos concursos específicos y un concurso general, en los que se han convocado 28 plazas (21 adjudicadas y 7 desiertas). Asimismo, se han provisto 8 puestos de trabajo en adscripción provisional.

En relación con la gestión de dotaciones, ya está planificada la convocatoria, durante 2025, de los oportunos procesos de provisión de puestos para la cobertura de las vacantes existentes.

En este sentido, la AEPD es consciente de la importancia de atraer y retener a los mejores profesionales, con una clara apuesta por el teletrabajo como doble instrumento, de ordenación del trabajo y de conciliación, compatibilizando la garantía del servicio a los intereses generales y el correcto ejercicio de sus competencias, con su compromiso con la igualdad y la corresponsabilidad, estableciendo medidas específicas para los trabajadores que tengan menores a su cargo para poder apoyar una maternidad y paternidad positivas.

Con ello, se alcanza un elevado grado de ocupación de los puestos de la entidad, debiendo destacarse la presencia femenina en los niveles directivos y predirectivos. Antes de la aprobación del Plan de Igualdad de la AEPD en 2020, la Agencia contaba con un 61,54% de hombres frente a un 38,46% de mujeres en dichos puestos.

A 31 de diciembre de 2024, dichos porcentajes se sitúan en un 51,33% de hombres frente a un 48,67% de mujeres, esto es, en tan solo 5 años se ha incrementado en 10 puntos la presencia femenina en los niveles directivos y predirectivos de la Agencia.

Durante 2024, la AEPD ha mantenido con fuerza las acciones formativas para su personal, con especial atención a las relacionadas con funciones de la AEPD, impartidas por formadores internos y externos en materias especializadas como la Inteligencia Artificial, criptografía o ciberseguridad.

6.2 Avance en digitalización

La AEPD continúa avanzando en la transformación digital de sus procesos y servicios para mejorar la calidad, la eficiencia y el desempeño satisfactorio de su cometido.

Durante el año 2024, la Secretaría General, a través de su departamento de tecnologías de la información, ha completado las actuaciones de digitalización y evolución de su infraestructura tecnológica, que se describen a continuación.

Con orientación al ciudadano, y a fin de facilitar su interacción con los servicios digitales ofrecidos y su experiencia de usuario, la Agencia ha abordado en este periodo diversos proyectos sobre su sede electrónica y los portales web.

Se puede destacar, en primer lugar, la evolución del buzón guiado de reclamaciones en la sede electrónica de la AEPD, dando lugar a la puesta en producción del conjunto de cuestionarios y formularios específicos para la presentación de las reclamaciones encuadradas en las categorías

de **Videovigilancia** y **Solicitudes de derechos no atendidas**, con sus subcategorías respectivas. El buzón guiado de reclamaciones tiene la finalidad de asistir al ciudadano en la presentación de las reclamaciones en materia de protección de datos, incorporando un cuestionario adaptado a cada subcategoría, que le orienta acerca de los pasos previos que se deben haber completado y las evidencias que son necesarias para su tramitación[1].

Por otra parte, con el objetivo de reducir cargas administrativas, se ha extendido el mecanismo desarrollado para incorporar archivos de mayor tamaño al delimitado por el servicio de registro, para ampliar, con las garantías debidas, el número de adjuntos admitidos en una misma presentación en sede electrónica.

Se ha llevado a cabo la actualización tecnológica del gestor de contenidos sobre el que se implementan los portales web "**Tú decides en internet**" y la **Red Iberoamericana de Protección de Datos** (en adelante, REDIPD), aprovechando para realizar un rediseño en profundidad, más moderno; optimizar su comportamiento en dispositivos móviles así como en relación con su posicionamiento SEO, y principalmente, mejorar su accesibilidad. Este último aspecto, en particular, ha sido auditado por un tercero independiente, que ha permitido incorporar en el pie de página un sello acreditativo del cumplimiento de los criterios de accesibilidad AA-WCAG 2.2.

Paralelamente al proyecto de actualización anterior, se han incorporado mejoras y funcionalidades remarcables tanto en el **Portal Institucional de la AEPD** como en el correspondiente a la REDIPD. En relación con el primero, se pueden señalar entre otras: la incorporación de sugerencias en los diversos buscadores, o la mayor facilidad en la aplicación de filtros de búsqueda mediante la activación y desactivación de *checkboxes*[2]; también, una sección renovada para la publicación de la información relativa a las convocatorias de puestos de trabajo, con un diseño que presenta la información de manera más estructurada y, por consiguiente, más clara.

Por su parte, el nuevo portal web de la REDIPD incluye ahora un buscador con diferentes facetas sobre un amplio repositorio documental.

Por último, cabe reseñar el desarrollo de nuevas versiones de los asistentes web al cumplimiento normativo, que se encuentran a disposición de responsables y encargados del tratamiento en el Portal Institucional, habiéndose migrado desde una plataforma propietaria a tecnología JavaScript (FACILITA RGPD, FACILITA EMPRENDE, Comunica-Brecha y Asesora-Brecha).

Las aplicaciones internas de gestión, en las que la Agencia se apoya para la tramitación electrónica de los procedimientos administrativos de su competencia, o la prestación de servicios internos, han sido también objeto de esfuerzo y actuaciones de mejora. En primer lugar, en lo que respecta al gestor en materia de reclamaciones de protección de datos, y a fin de lograr mayor agilidad e incrementar la eficiencia ante el aumento de solicitudes, se ha continuado ahondando en la automatización de aquellas tareas y flujos susceptibles de una realización desasistida; y se han incorporado además funcionalidades como la gestión dinámica y flexible de reglas para la asignación automática de entradas. Por otro lado, la aplicación ofrece ahora la capacidad de configuración de alertas personalizables por usuario y un sistema para la difusión de novedades o intervenciones. Asimismo, permite el intercambio de escritos vinculados a procedimientos judiciales, mediante el mecanismo definido por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes para la **comunicación entre Administraciones Públicas y los Órganos Judiciales**, o el envío de peticiones de firma directamente a cargos.

En cuanto al tramitador corporativo que da soporte al resto de procedimientos y servicios competencia de la AEPD, cabe reseñar la evolución sustancial que ha experimentado, ofreciendo una mayor potencia, facilidad y flexibilidad en la elaboración de documentos, y la integración de nuevos servicios de registro, sellado y notificación que han permitido, por ejemplo, una gestión íntegra de los posibles casos de uso en la notificación.

---

[1] *Evidencias y requisitos de admisibilidad establecidos mediante Resolución de 29 de junio de 2023, de la Dirección de la Agencia Española de Protección de Datos, por la que se aprueban los modelos de presentación de reclamaciones.*

[2] *Del inglés, casillas de verificación.*

De igual modo, se ha abordado y completado un proyecto de largo recorrido con el objetivo de la actualización tecnológica y refactorización de la Plataforma de Administración electrónica de la Agencia, que aglutina un extenso conjunto de servicios y actúa como nodo de interoperabilidad entre las aplicaciones de gestión de la AEPD y los servicios transversales que presta la Secretaría General de Administración Digital[3] (registro, notificaciones, firma y sellado, representación, etc.). Este proyecto se ha paralelizado, adicionalmente, con el desarrollo y puesta a disposición en la mencionada Plataforma, de nuevos servicios para la gestión directa de las notificaciones y comunicaciones postales con el centro de impresión y ensobrado empleado.

En su compromiso por la mejora continua, el departamento de tecnologías de la información ha seguido apostando por la automatización e implantación de procesos y herramientas que aseguren una mayor calidad y seguridad de los desarrollos llevados a cabo, alcanzando un mayor grado de madurez en su desempeño. Con esta finalidad, se ha promovido la puesta en marcha de una Oficina de calidad, desde la que se han elaborado guías técnicas que describen el ciclo de vida de desarrollo y la arquitectura de integración y despliegue continuos (CI/CD) que se ha adoptado, para su estandarización y aplicación en todos los proyectos.

Las iniciativas de actualización y modernización se han impulsado también en el área de la infraestructura de sistemas y comunicaciones, en aras de su homogeneización, aseguramiento de la continuidad y disponibilidad, la seguridad y, en su conjunto, la mejora en la prestación del servicio. A modo de ejemplo, se ha abordado la actualización de las bases de datos y el gestor documental a las últimas versiones disponibles o el incremento de la velocidad de acceso en la conexión de la Agencia a la red que cursa el tráfico de datos. Al mismo tiempo, se ha proseguido con las actuaciones dirigidas a la homogeneización del sistema operativo y *middleware*[4] y securización de los servidores, bastionados de conformidad con las directrices CCN-STIC[5], en el marco de un proyecto iniciado el año anterior. Beneficio derivado de este último, ha sido la posibilidad de automatizar tareas de administración, lo que ha comportado ahorro en tiempo y reducción de errores.

También a efectos de disminuir el esfuerzo en mantenimiento, y con un acceso más inmediato a las últimas funcionalidades, se ha optado por el uso de los servicios transversales y horizontales en sus versiones *cloud*[6], acometiendo en el curso de este año el proyecto de migración hacia NEDAES en la nube y Nómina Centralizada, desde sus versiones *on-premise*[7].

Como iniciativa más relevante en este ámbito, se ha acordado el uso de la solución compartida de nube híbrida NubeSARA, proporcionada por la SGAD, para alojar la infraestructura de sistemas y aplicaciones de la Agencia. Acompañado de la firma del convenio pertinente entre las partes para la prestación del servicio, se han iniciado los trabajos de migración, que se extenderán hasta comenzado el 2025.

La mejora en la retransmisión de eventos y celebración de webinarios y videoconferencias es un objetivo permanente, en atención al cual se ha renovado el equipamiento audiovisual principal

---

[3] La Secretaría General de Administración Digital (o SGAD), dependiente hasta la fecha del Ministerio para la Transformación Digital y de la Función Pública, es el órgano directivo encargado de impulsar el proceso de racionalización de las tecnologías de la información y de las comunicaciones en el ámbito de la Administración General del Estado y sus Organismos Públicos. Actualmente, se encuentra en proceso de transformación en la Agencia Estatal de Administración Digital, tras la aprobación de su Estatuto mediante el RD 1118/2024, de 5 de noviembre.

[4] Middleware, o software que se sitúa entre el sistema operativo y las aplicaciones, y que proporciona servicios y funciones comunes.

[5] Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones.

[6] "Cloud", del inglés, aplicable en este contexto a plataformas, aplicaciones o servicios que son alojados y proporcionados por un proveedor externo, y puestos a disposición vía internet (u otra red de comunicaciones).

[7] "On-premise", del inglés, referido a infraestructura o sistemas software alojados en instalaciones o ubicaciones propias.

para lograr un uso más intuitivo y sencillo. Con el mismo fin, se ha procedido a la reubicación del armario de control de los sistemas audiovisuales, cámaras e iluminación en el Salón de Actos. La organización de los diferentes eventos y webinarios cuenta además con el soporte y atención por parte del departamento de Tecnologías tanto para su preparación como durante la realización de éstos.

De igual modo, se ha mantenido el esfuerzo orientado a la mejora en la labor continua de atención y soporte al usuario.

En el ámbito de la ciberseguridad, acorde con su cada vez mayor relevancia, dedicación y atención necesaria por parte de las organizaciones, se han acometido actuaciones significativas, en colaboración en su caso con otras áreas del departamento, que han redundado en la mejora de la prevención y detección de posibles amenazas y vulnerabilidades, así como en el incremento de la seguridad de los sistemas y servicios.

En relación con las redes de comunicaciones, se han impulsado y llevado a término varios proyectos paralelamente que han incrementado y mejorado sustancialmente su seguridad, comprendiendo actuaciones encaminadas tanto al control del flujo del tráfico (segmentación de VLAN y túneles VPN, depuración de reglas en *firewalls*[8]) como al refuerzo en el acceso y autenticación de equipos y usuarios (doble factor, autenticación de equipos mediante certificado, o comprobación de la "salud" de los equipos que se conectan; etc.)

Asimismo, se han implantado soluciones que han permitido extender la protección de activos tales como las aplicaciones y servicios de la AEPD disponibles en internet, el correo, o los equipos de usuarios, proporcionando salvaguardas frente a amenazas, adicionales o complementarias a otros sistemas ya en funcionamiento.

También se ha promovido la realización de pruebas de penetración de diversos tipos (intrusión o auditorías de *ransomware*[9], pentesting de caja negra/caja blanca de servicios, etc.), o el análisis de seguridad de nuevas versiones de aplicaciones, por auditores externos, que han permitido priorizar las tareas de eliminación y mitigación de vulnerabilidades.

A lo largo de este año se ha continuado con la adopción decidida de los servicios de prevención y detección puestos a disposición tanto por el Centro de Operaciones de Ciberseguridad de la AGE (COCS) como el Centro Criptológico Nacional (CCN). Y en un contexto normativo, se ha trabajado en la definición y redacción de procedimientos e instrucciones de seguridad.

Por último, se ha mantenido la apuesta por la concienciación en ciberseguridad de todo el personal, mediante un curso interactivo y "a su ritmo" que incorpora nuevos módulos y contenidos de forma periódica, y que se ha complementado con la realización de campañas de simulación de phishing[10].

6.3 Eficiencia en la gestión de los recursos

La gestión económica y financiera de un organismo público como la AEPD requiere una planificación detallada y una administración eficiente de sus recursos.

En el año 2024 el presupuesto inicial de gastos de la AEPD ha ascendido a 18.750.730 euros, resultado de la prórroga para 2024 de los Presupuestos Generales del Estado de 2023.

[8] Firewall, del inglés, dispositivo de seguridad de red diseñado para monitorizar, filtrar y controlar el tráfico de red entrante y saliente, con base en reglas predeterminadas.

[9] Ransomware, software malicioso que secuestra y restringe el acceso a un sistema o información, exigiendo un pago económico a la víctima.

[10] Phishing, conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza, para manipularla y lograr que realice acciones perjudiciales para ésta (proporcionar datos personales, bancarios, etc.).

Para hacer frente a las necesidades presupuestarias de gastos de personal durante el ejercicio 2024, se realizó una variación presupuestaria por importe de 1.537.659,88 euros.

Como en anteriores ejercicios, el nivel de ejecución presupuestaria se ha mantenido muy alto, concretamente, en un 96,0% para el año 2024.

En relación con la ejecución de su presupuesto de ingresos, a 31 de diciembre de 2024 el importe de los derechos reconocidos brutos ascendió a 45.795.030,32 euros, de los que un 96% (43.739.510,82) corresponden a derechos reconocidos por sanciones. Tras contabilizar las insolvencias o anulaciones producidas durante el año, el importe de los derechos reconocidos netos ha quedado establecido en 38.424.004,70 euros.

Los derechos reconocidos representan el conjunto de los ingresos que la AEPD tiene derecho a percibir, hayan sido o no efectivamente recaudados.

La recaudación total de derechos reconocidos en el ejercicio corriente 2024 asciende a 23.206.285,33 euros, de los que 21.150.765,83 euros corresponden a sanciones (un 91%). Tras contabilizar la devolución de sanciones por importe de 543.681,34 euros, la recaudación neta en 2024 de derechos reconocidos en el ejercicio corriente ha sido de 20.607.084,49 euros.

Adicionalmente, al sumar la recaudación de derechos pendientes de cobro, reconocidos en ejercicios anteriores; la recaudación total de sanciones en el año 2024 asciende a 29.328.785,44 euros brutos y 28.785.104,10 euros netos, tras contabilizar las devoluciones.

En el año 2024 se han pagado 61.533,83 euros de intereses de demora como consecuencia de la estimación total o parcial de recursos potestativos de reposición o contencioso-administrativos.

En cuanto al resto de ingresos, los conceptos más significativos en el año 2024 se corresponden con la generación de ingresos financieros de 2.032.706,96 euros por intereses de cuentas bancarias, el reintegro de gastos por instituciones de la Unión Europea 15.803,38 euros (capitulo 4) y el reintegro de anticipos al personal de 7.009,16 euros (capítulo 8).

7. La necesaria cooperación institucional

7.1 Consejo Consultivo

El Consejo Consultivo de la Agencia, órgano colegiado de asesoramiento de la Presidencia, se reunió en 2024 en dos ocasiones.

En la reunión del 17 de julio se puso de manifiesto el gran incremento de actividad de la AEPD en todas sus subdirecciones y divisiones, destacando el foco en menores, salud digital y privacidad, iniciativa valorada muy positivamente por los miembros del Consejo.

En la reunión del 10 de diciembre, además de exponer la actividad de las distintas unidades, se fallaron los Premios Protección de Datos 2024.

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 la sede de la Agencia, 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 marco de la necesaria cooperación institucional con las autoridades autonómicas de protección de datos, la AEPD mantuvo en el mes de febrero de 2024 una primera reunión con representantes de la Autoridad Vasca de Protección de Datos (AVPD), la Autoridad Catalana de Protección de Datos (APDCAT) y el Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA).

En dicha reunión se debatieron diferentes asuntos, como la actualización de la guía de cookies; las propuestas de actuaciones para la protección de los menores en internet; los Sistemas de verificación de edad; los criterios de actuación ante las plataformas educativas y de aprendizaje y las herramientas digitales.

También se despacharon otras cuestiones relacionadas con actuaciones sobre el tratamiento de datos biométricos, así como los criterios para determinar la cuantía de algunas sanciones y se compartió información de ciertos procesos de investigación.

Asimismo, se abordaron otras cuestiones relacionadas con la gestión de brechas de seguridad y los criterios sobre su tramitación y se aprovechó la reunión para actualizar la información resultante de las reuniones con el EDPB.

En el mes de noviembre se mantuvo una reunión virtual y presencial con todas las Autoridades Autonómicas de Protección de Datos, organizada en esta ocasión por el Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA).

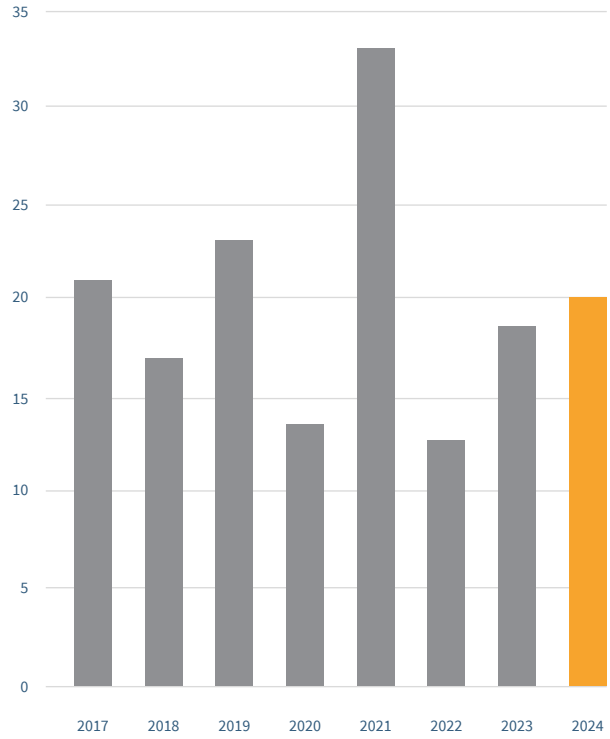
Asimismo, se realizó una coordinación sobre criterios establecidos en materia de brechas de seguridad de datos personales.

Por otro lado, también en 2024 se han celebrado dos reuniones en el marco de los Espacios de Estudios de IA y a iniciativa de la autoridad andaluza, se celebró una reunión de creación del Espacio de Estudios de Genética.

7.3 Relaciones con el Defensor del Pueblo

Durante el año 2024 se han tramitado un total de 20 asuntos, frente a los 18 de 2023.

Evolución quejas DP



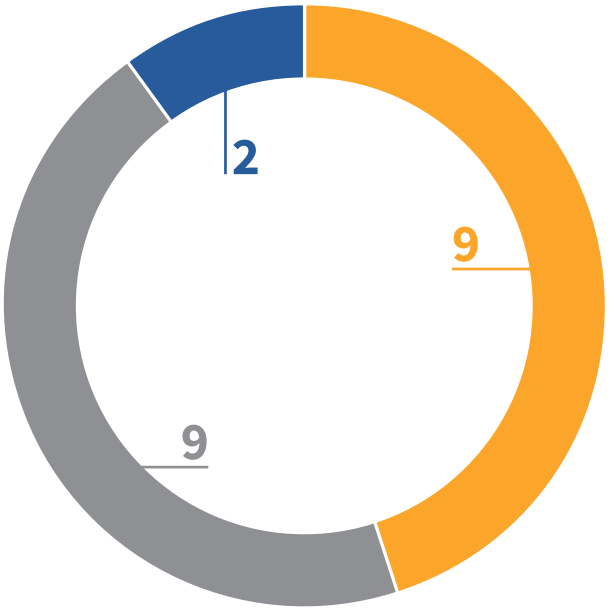
Respecto a los motivos que han llevado a la ciudadanía a dirigirse a la AEPD mediante este cauce, prácticamente en la mitad de los casos, lo han sido para solicitar información sobre el estado de tramitación de su denuncia (captura de imagen de documento identificativo por agente de la autoridad y estafas cometidas mediante la suplantación de la identidad) o falta de resolución en tiempo del recurso presentado ante la Agencia.

En la mayoría de los escritos remitidos por el Defensor del Pueblo se solicita a la AEPD que inicie actuaciones sobre los hechos objeto de la queja enviada, que profundice en su estudio o bien que fije un criterio en relación con algunos de los asuntos planteados.

En otros casos, se repite la misma solicitud requiriendo la ampliación de la información remitida en su momento por parte de esta Agencia en relación a las quejas presentadas sobre el ejercicio del derecho de acceso ante el Ministerio del Interior, por parte de las personas solicitantes de protección internacional, en concreto respecto a su Número de Identificación de Extranjeros (NIE), registradas por la Policía y la comunicación de datos por la dirección general de política interior a la policía y a la tesorería general de la seguridad social.

- Ausencia de respuesta AEPD
- Solicitud de información por el DP
- Otras solicitudes de información

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 Agencia ha **participado de forma muy activa** en el Comité Europeo de Protección de Datos a lo largo del año 2024. La Agencia está representada en todos los subgrupos de expertos del Comité Europeo de Protección de Datos **y ha actuado como redactor principal o corredactor** en varios de los documentos que el Comité ha publicado en 2024.

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 2024 CEPD **ha aprobado las siguientes Directrices**:

Directrices 1/2023: Sobre el artículo 37 de la Directiva policial (680/2016) (aprobadas en 2024)

Estas directrices aportan garantías adecuadas para Transferencias Internacionales en materia de cooperación policial y judicial a terceros estados en ausencia de una decisión de adecuación de la Comisión Europea. Estas garantías adecuadas pueden lograrse mediante un instrumento legalmente te vinculante o, en su defecto, a través de una evaluación detallada por parte del responsable del tratamiento

Las directrices también enfatizan la importancia de que los Estados miembros, al negociar acuerdos internacionales que impliquen transferencias de datos personales, aseguren que dichos acuerdos contengan salvaguardas que ofrezcan una protección esencialmente equivalente a la proporcionada por la Directiva. Además, se subraya el papel crucial de las autoridades de supervisión nacionales en la evaluación y supervisión de estas transferencias para garantizar el cumplimiento de las normativas de protección de datos.

En resumen, estas directrices buscan garantizar que las transferencias internacionales de datos personales en el ámbito de la aplicación de la ley se realicen con un nivel de protección adecuado, preservando los derechos fundamentales de las personas en relación con sus datos personales.

Estas directrices fueron sometidas a consulta pública tras lo cual se aprobaron en 2024 en su versión definitiva disponible en el siguiente **enlace**.

Directrices 2/2023: Sobre el alcance técnico del Art. 5(3) de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva 2002/58/EC, ePrivacy) (aprobadas en 2024)

El objetivo de estas directrices es realizar un análisis técnico sobre el ámbito de aplicación del artículo 5 apartado 3 de la Directiva europea sobre la privacidad y las comunicaciones electrónicas (Directiva ePrivacy). En concreto pretenden aclarar qué se entiende por almacenamiento o acceso a información almacenada en el equipo terminal de un suscriptor o usuario. Las directrices no abordan las circunstancias bajo las cuáles una operación de tratamiento puede estar dentro de las excepciones del requisito de consentimiento previstas por la Directiva.

La aparición de nuevos métodos de seguimiento para reemplazar las herramientas de rastreo existentes (por ejemplo, las cookies, debido a la interrupción del soporte a las cookies de terceros) y la creación de nuevos modelos de negocio se ha convertido en una preocupación crítica en materia de protección de datos. Si bien la aplicabilidad del artículo 5 apartado 3 de la Directiva sobre privacidad electrónica está claramente establecida para algunas tecnologías de seguimiento, como por ejemplo las cookies, es necesario eliminar las ambigüedades relacionadas con la aplicación de dicha disposición a las herramientas de seguimiento emergentes, como pueden ser los píxeles y urls de seguimiento, el seguimiento basado en la dirección IP, el procesamiento local y los identificadores únicos entre otras.

Estas directrices fueron sometidas a consulta pública tras lo cual se aprobaron en 2024 en su versión definitiva disponible en el siguiente **enlace**.

Directrices 1/2024: Sobre el tratamiento de datos personales basados en el art.6.1. f del RGPD.

Su objetivo: analizar los requisitos establecidos en el artículo 6, apartado 1, letra f), del RGPD que deben cumplir los responsables para que el tratamiento de datos personales sea licito y «necesario para la satisfacción de los fines de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero».

Las directrices abordan los siguientes **aspectos claves**:

1. Elementos que se deben tener en cuenta para aplicar el 6.1.f del RGPD como base legal del tratamiento: En este apartado se ofrecen una serie de criterios y recomendaciones para que los responsables del tratamiento puedan

evaluar y documentar si se cumplen estas tres condiciones acumulativas: Respecto a la primera condición relativa a la "persecución de un interés legítimo", se define el concepto interés frente a la finalidad del tratamiento. No todos los intereses del responsable del tratamiento o de un tercero pueden considerarse legítimos; solo los intereses lícitos, definidos con precisión y claridad, que sean reales (no especulativos) pueden invocarse válidamente para aplicar el artículo 6, apartado 1, letra f), del RGPD como base jurídica.

Por lo que respecta a la segunda condición, de que el tratamiento de datos personales sea "necesario para los fines de los intereses legítimos perseguidos", se señalan los elementos objetivos que el responsable ha de tener en cuenta para comprobar si los intereses legítimos perseguidos no pueden ser razonablemente alcanzados con la misma eficacia por otros medios menos restrictivos de los derechos y libertades fundamentales de los interesados.

Finalmente, y por lo que respecta a la tercera condición de que "los intereses o los derechos y libertades fundamentales de la persona afectada por el tratamiento de datos no prevalezcan sobre los intereses legítimos del responsable del tratamiento o de un tercero", este requisito implica una ponderación de los derechos e intereses en conflicto que depende, en principio, de las circunstancias específicas del tratamiento de que se trate.

2. Relación del art.6.1. f del RGPD con los demás derechos de los interesados.

3. Aplicación contextual del art.6.1. f del RGPD: describe varios contextos específicos en los que podría invocarse el artículo 6, apartado 1, letra f), del RGPD, o que presentan características singulares que deben tenerse muy en cuenta a la hora de ponderar los distintos intereses y derechos y libertades fundamentales en juego.

Estas directrices fueron adoptadas el 8 de octubre de 2024 y sometidas a consulta pública que finalizó el 20 de noviembre de 2024. Disponible en el siguiente **enlace**.

Directrices 02/2024: Sobre el art.48 del RGPD

Estas directrices ofrecen orientación sobre la aplicación del Artículo 48 del RGPD. Este artículo aborda las condiciones bajo las cuales las decisiones y resoluciones de autoridades de terceros países que requieren la transferencia o divulgación de datos personales pueden ser reconocidas y ejecutadas en la Unión Europea.

Estas directrices señalan que para poder aplicar correctamente el art.48 del RGPD, primero hay que ver si existe un acuerdo internacional, y en el caso de que existiera debería comprobarse además que contenga bases legales del art 6.1.c (en cumplimiento de una obligación legal) y del art.6.1.e del RGPD (en cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos) y que cumpla además con los requisitos legales exigidos en el Capítulo V del RGPD, por lo que la mera existencia de un acuerdo internacional no es por sí misma una condición suficiente ni un prerrequisito excluyente, ya que puede que este acuerdo no contenga las bases legales citadas anteriormente o no contenga las garantías adecuadas.

No obstante, la interpretación que se realiza del art. 48 del RGPD permite que, incluso en ausencia de un acuerdo internacional, puedan realizarse transferencias en aplicación de otras bases legales como son las Decisiones de Adecuación o las excepciones del art.49 del RGPD para que la sentencia o la decisión administrativa de un tercer país pueda ser reconocida o ejecutable.

Estas directrices fueron adoptadas en el Plenario de 2 de diciembre de 2024 y fueron sometidas a consulta pública. Disponible en el siguiente **enlace**.

Directrices 1/2025: sobre pseudonimización

La pseudonimización es un mecanismo que permite reducir los riesgos para los titulares de datos al evitar la atribución directa de la información personal a individuos específicos sin el uso de información adicional. Aunque la pseudonimización no es obligatoria bajo el RGPD, se recomienda como una medida efectiva para cumplir con principios clave como la minimización de datos, la protección por diseño y por defecto, y la seguridad de la información.

Este proceso se basa en transformar los datos de modo que solo puedan vincularse a una persona mediante información adicional que debe mantenerse separada y protegida. Sin embargo, los datos pseudonimizados siguen considerándose datos personales si pueden atribuirse a un individuo mediante medios razonablemente accesibles. Para garantizar su efectividad, es crucial definir un "dominio de pseudonimización", es decir, el contexto en el cual la atribución de los datos está restringida a ciertos actores autorizados.

Entre sus beneficios, la pseudonimización puede facilitar el análisis de datos sin comprometer la privacidad, reducir el impacto de posibles brechas de seguridad y permitir transferencias internacionales de datos de manera más segura. No obstante, por sí sola no garantiza el anonimato ni exime del cumplimiento del RGPD. Su implementación debe ir acompañada de otras medidas técnicas y organizativas que refuercen la protección de los datos y aseguren que la información adicional necesaria para la reidentificación no sea accesible a partes no autorizadas.

Estas directrices han sido sometidas a consulta pública en la versión disponible en el siguiente **enlace**, estando pendiente de publicación la versión definitiva.

DICTÁMENES

Dictamen 05/2024, sobre el proyecto de decisión de la Autoridad de Supervisión española relativo a las Normas Corporativas Vinculantes del Responsable de Tratamiento del Grupo MAPFRE

El CEPD ha emitido su dictamen sobre la decisión preliminar de la Autoridad de Supervisión Española respecto a las Normas Corporativas Vinculantes para Responsables del Tratamiento (BCR-C) del Grupo MAPFRE. Estas normas permiten la transferencia de datos personales fuera del Espacio Económico Europeo (EEE), garantizando un nivel adecuado de protección conforme al RGPD.

El CEPD evaluó la conformidad de las BCR-C de MAPFRE con los requisitos del artículo 47 del RGPD y sus recomendaciones sobre la aprobación de dichas normas. La evaluación confirmó que el documento presentado cumple con los criterios exigidos, asegurando salvaguardias adecuadas para la protección de los datos transferidos a países terceros. No se identificaron preocupaciones que requirieran ajustes en la propuesta. Las BCR-C de MAPFRE cubren datos de empleados, clientes, candidatos, representantes empresariales, proveedores y otros interesados.

El CEPD concluyó que la decisión preliminar de la AEPD puede adoptarse sin modificaciones. Sin embargo, destacó que la aprobación de las BCR-C no implica la validación automática de transferencias específicas a terceros países si no se garantiza un nivel de protección equivalente al de la UE. Asimismo, recordó las condiciones bajo las cuales MAPFRE puede actualizar sus normas, incluyendo la modificación de la lista de entidades adheridas.

Este dictamen se adoptó por el Comité en el Plenario de 14 de marzo de 2024. Disponible en el siguiente **enlace**.

Dictamen 08/2024, sobre consentimiento válido en el contexto de los modelos Consiente o Paga utilizados por las grandes Plataformas on line.

A raíz de la Sentencia del TJUE *Meta vs Bundeskartellamt* (asunto C-252/21) y ante la disparidad de criterios interpretativos por parte de las DPA nacionales y el uso cada vez más frecuente por parte de las webs del modelo "*consiente o paga*", el EDPB decidió adoptar este Dictamen dirigido a grandes plataformas en línea.

Efectivamente, la citada Sentencia del TJUE *Meta vs Bundeskartellamt* parece indicar que el modelo «consent or pay» no estaría prohibido en principio, pero no proporciona detalles sobre cómo funcionaría en la práctica. En este sentido, el CEPD interpreta la citada sentencia en el sentido de que el modelo "*consent or pay*" está permitido con carácter general siempre que se respeten los requisitos del RGPD para un consentimiento válido, sometido a evaluación teniendo en cuenta las circunstancias del caso concreto y del propio tratamiento, de forma que a los usuarios que no presten su consentimiento se ofrezca, si es necesario a cambio de una tasa adecuada, una alternativa equivalente que no vaya acompañada de tales operaciones de tratamiento de datos.

Con este dictamen se pretende identificar una serie de conceptos y criterios comunes sobre los modelos de Consiente o Paga que serán objeto del correspondiente desarrollo posterior en las futuras directrices sobre los citados modelos que se encuentran en fase de elaboración como son: "*la alternativa equivalente*" que no vaya acompañada de tratamiento de datos, con o sin tasa; "*la tercera alternativa*" (*Free Alternative Without Behavioural Advertising*) que sería un servicio gratuito, sin incluir el tratamiento de los datos personales de los usuarios para la publicidad conductual, pero que sí permite que puedan tener lugar otras formas de publicidad como la publicidad contextual o la publicidad general basada en temas, menos intrusiva para la privacidad; o la "*tasa apropiada*» que aunque el TJUE en su sentencia no aporta elementos adicionales a este respecto, en el dictamen se recuerda el principio general de que el derecho a la protección de datos no implica que el interesado deba pagar para poder disfrutar de este derecho y que los datos personales no son una mercancía negociable. Por otra parte, se reconoce que las empresas son libres de fijar sus propios precios y que debe respetarse la libertad de empresa.

Este dictamen se adoptó por el Comité en el Plenario de 17 de abril de 2024. Disponible en el siguiente **enlace**.

Dictamen 28/2024, sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de Inteligencia Artificial (IA)

A petición de la autoridad de protección de datos irlandesa (DPC) el Comité emitió este Dictamen sobre el tratamiento de datos personales en el desarrollo y despliegue de modelos de IA. Se analiza en qué condiciones un modelo de IA puede considerarse anónimo, los criterios para validar el interés legítimo como base legal para su desarrollo y despliegue, y las consecuencias del tratamiento ilegal de datos personales en la fase de desarrollo.

Un modelo de IA entrenado con datos personales no puede considerarse anónimo en todos los casos. La evaluación debe realizarse caso por caso, considerando la posibilidad de extracción directa o indirecta de datos personales del modelo. Para demostrar la anonimización, se deben implementar medidas que limiten la reidentificación y documentar los controles aplicados.

El interés legítimo puede servir como base legal para el tratamiento de datos personales en la creación y despliegue de modelos de IA, siempre que se cumplan tres condiciones: la finalidad del tratamiento debe ser legal, claramente definida y actual; la necesidad del tratamiento debe justificarse sin alternativas menos intrusivas; y el interés del responsable no debe prevalecer sobre los derechos fundamentales de los interesados.

El uso ilegal de datos personales en la fase de desarrollo puede afectar la legalidad del procesamiento posterior. Si los datos personales permanecen en el modelo, las autoridades deben evaluar si el desarrollo y despliegue constituyen

actividades separadas. Cuando un modelo ha sido desarrollado con datos tratados ilegalmente y luego anonimizado, el procesamiento posterior no se vería afectado, salvo que vuelvan a procesarse datos personales en fases posteriores.

Este dictamen se adoptó por el Comité en el Plenario de 18 de diciembre de 2024. Disponible en el siguiente **enlace**.

DECLARACIONES

Declaración 1/2024 sobre la evolución legislativa en relación con la Propuesta de Reglamento por el que se establecen disposiciones para prevenir y combatir el abuso sexual infantil

El CEPD reconoce la importancia de combatir el abuso sexual infantil en línea y valora las mejoras propuestas por el Parlamento Europeo en la regulación destinada a este fin. Sin embargo, expresa preocupaciones sobre la posible vulneración de los derechos fundamentales a la privacidad y la protección de datos.

El CEPD destaca la exclusión de las comunicaciones cifradas de extremo a extremo de las órdenes de detección y la eliminación de la obligación de analizar audio y texto. No obstante, advierte que persisten problemas significativos, especialmente en relación con la vigilancia generalizada e indiscriminada de las comunicaciones privadas. Se cuestiona la falta de claridad en los criterios para emitir órdenes de detección y la posibilidad de que estas afecten a personas sin una vinculación comprobada con el abuso infantil. También alerta sobre el uso de tecnologías para identificar material nuevo de abuso infantil debido a sus altas tasas de error, lo que podría generar acusaciones injustificadas. El CEPD subraya la necesidad de preservar el cifrado de extremo a extremo, y recomienda que la propuesta de reglamento incluya evaluaciones de impacto rigurosas para garantizar que las medidas propuestas sean necesarias y proporcionales, minimizando cualquier posible intrusión en la privacidad de los individuos, garantizado los derechos fundamentales de las personas. Esta declaración se encuentra disponible en el siguiente **enlace**.

Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco del Reglamento europeo de Inteligencia Artificial

El CEPD destaca la importancia del papel de las autoridades de protección de datos (DPAs) en el marco del Reglamento de Inteligencia Artificial. Dado que este reglamento regula la comercialización y el uso de sistemas de IA en la UE, debe interpretarse en conjunto con la normativa de protección de datos, ya que el tratamiento de datos personales es un componente clave en muchas aplicaciones de IA, especialmente en aquellas de alto riesgo.

El CEPD recomienda que los Estados miembros designen a las DPAs como autoridades de vigilancia de mercado para los sistemas de IA de alto riesgo, en particular en áreas sensibles como el cumplimiento de la ley, la gestión fronteriza, la justicia y los procesos democráticos. Esto garantizaría coherencia regulatoria y un punto de contacto único para empresas y ciudadanos. Además, subraya la necesidad de establecer mecanismos claros de cooperación entre las DPAs y otras autoridades reguladoras para evitar contradicciones en la aplicación de normas.

También se enfatiza que cualquier sistema de IA que implique el procesamiento de datos personales debe estar sujeto a la supervisión de las DPAs. Asimismo, el CEPD insta a la Comisión Europea y a la Oficina de IA de la UE a coordinarse con las DPAs para garantizar una aplicación armonizada del Reglamento de IA, respetando plenamente los derechos fundamentales a la privacidad y la protección de datos.

Esta declaración se encuentra disponible en el siguiente **enlace**.

8.1.2 Grupo de trabajo (Taskforce) sobre ChatGPT

Durante 2024 este grupo de trabajo ha mantenido reuniones periódicas intercambiando información y sirviendo de mecanismo de coordinación entre las autoridades de control, para armonizar las decisiones a tomar sobre este servicio.

Desde el 15 de febrero de 2024 Open AI (entidad norteamericana propietaria del servicio) ya dispone de un establecimiento dentro del EEE, por lo que es posible el denominado mecanismo de ventanilla única del RGPD, también conocido como One-Stop-Shop, o OSS, por sus siglas en inglés. Este mecanismo OSS proporciona un canal formal de coordinación entre las autoridades de control concernidas en cada expediente para acordar en concertación los borradores de decisiones relativos a tratamientos transfronterizos de datos.

Por esta razón a finales de 2024 se da por concluida el cometido de coordinación de autoridades bajo este grupo de trabajo, que seguirá temporalmente vigente en el ámbito de los casos concretos abiertos.

8.1.3 Grupo de trabajo (Taskforce) sobre competencia, consumo y protección de datos

Se han celebrado **cinco reuniones** de este grupo durante 2024.

Se decidió por parte del grupo designar puntos de contacto nacionales en las autoridades de consumo y competencia para llevar a cabo el desarrollo de los trabajos. La AEPD tiene ya puntos de contacto nacional en la CNMC y en la Oficina de Enlace Única para la Cooperación para la Protección al Consumidor (CPC) de la Dirección General de Consumo (Ministerio de Derechos Sociales, Consumo y Agenda 2030). Se han producido reuniones con los vocales designados para esta cooperación y la AEPD se viene sumando a las reuniones de la CNMC y la CPC en foros internacionales.

A finales de 2024 el CEPD decidió dar potenciar y dar continuidad a este grupo de trabajo dándole carácter permanente, en forma de un nuevo subgrupo de expertos denominado Cross-Regulatory Interplay and Cooperation (Cooperación e Interacción Interreguladora).

8.1.4 Grupo de Alto Nivel para la aplicación de la Ley de Mercados Digitales de la Unión Europea

La AEPD forma parte, como uno de los representantes del Consejo Europeo de Protección de datos, en el Grupo de Alto Nivel de la Comisión Europea sobre la aplicación del Reglamento europeo 2022/1925 de Mercados Digitales (DMA).

Este grupo cuenta con dos subgrupos especializados, uno dedicado a las obligaciones establecidas en el artículo 5 (Obligaciones de los guardianes de acceso) y otro dedicado a las obligaciones establecidas en el artículo 7 (Obligación de los guardianes de acceso en materia de interoperabilidad de los servicios de comunicaciones interpersonales independientes de la numeración) del citado reglamento.

Durante 2024 la AEPD ha participado en **dos reuniones anuales** del subgrupo del artículo 5 y otras dos reuniones anuales del subgrupo del artículo 7.

8.2 La cooperación con Iberoamérica

Actividades de la Red Iberoamericana de Protección de Datos (RIPD)

8.2.1 Reunión grupos de trabajo RIPD 1 al 3 de abril, Lima (Perú)

La reunión de estos grupos de trabajo concluyó con un gran éxito de participación y un alto grado de objetivos cumplidos. Asistieron representantes de 10 países de Europa y de la Región Iberoamericana y se reforzaron alianzas entre las Autoridades de Protección de Datos en el marco de la Red y de los Grupos de Trabajo, promoviéndose el desarrollo de una agenda de trabajo común para una convergencia regulatoria.

Durante los días que se celebraron las reuniones se desarrollaron Mesas de Trabajo en las que se abordó el estado actual de investigaciones

iniciadas sobre la actividad de empresas desarrolladoras de inteligencia artificial y su incidencia sobre los datos personales. También se concretaron acciones para frenar la violencia digital y promover la salud digital, así como para prevenir los efectos de la violación de los derechos de protección de datos personales por la acción de empresas dedicadas a su recopilación y tratamiento: iris y datos biométricos. Hubo una mesa dedicada a discutir la convergencia de estándares de protección de datos en la Región y la aplicación práctica de las cláusulas contractuales modelo, para facilitar el flujo de datos transfronterizos. El 2 de abril se llevó a cabo la Conferencia Internacional "La Protección de Datos Personales Frente a los Desafíos Contemporáneos", que contó con la asistencia de más de 500 personas y se trataron temas como la "Regulación internacional de la inteligencia artificial"; "Los nuevos desafíos para los derechos frente al avance de la neurociencia"; "Actualizaciones normativas en la región para la protección de datos personales"; y "Menores, privacidad y seguridad digital".

8.2.2 Firma de la Carta de Intenciones UNESCO-RIPD

En el mes de julio de 2024 se firmó una Carta de Intenciones entre la UNESCO y la RIPD, en la que se plasmó una colaboración en materia de Inteligencia Artificial, Neurotecnologías, Violencia Digital y Salud Digital.

Como resultado de esta Carta de Intenciones, los países miembros de la RIPD participaron en la Recomendación UNESCO sobre Ética de las Neurotecnologías.

8.2.3 Firma Memorándum de Entendimiento SEGIB-RIPD

También en el mes de julio de 2024, en el marco de la Carta Iberoamericana de Principios y Derechos en Entornos Digitales (CIPDED), se actualización los estándares iberoamericanos, se diseñaron e implementaron políticas públicas en materia de protección de datos alineadas con los desafíos actuales (IA, neurotecnologías) y se identificaron sus consecuencias en la privacidad de la ciudadanía, en especial en los colectivos más vulnerables (Salud Digital/Menores).

El informe se presentó en la XXIX Cumbre Iberoamericana de Jefas y Jefes de Estado y de Gobierno celebrada en el mes de noviembre de 2014 en la ciudad de Cuenca (Ecuador), bajo el lema: "Innovación, Inclusión y Sostenibilidad".

8.2.4 Encuentro RIPD 2024: 27 al 29 de mayo, Cartagena de Indias (Colombia)

En el contexto actual de fuerte digitalización social, la RIPD ha creído necesario actualizar su Reglamento interno con el fin de afrontar los nuevos retos de manera más eficiente. Con motivo de este Encuentro, se aprobaron una serie de cambios de redacción. Asimismo, se aprobó y dio la bienvenida a los nuevos miembros y observadores.

Se avanzó en la colaboración entre autoridades de protección de datos y en el incremento del intercambio de información y la visibilidad de la RIPD.

En materia de Inteligencia Artificial se destacó la importancia de la IA para el desarrollo económico y social y el fuerte impacto que la implantación desregulada de esta tecnología puede tener para el derecho a la protección de datos personales. Se abogó por una regulación equilibrada que fomente el desarrollo de esta tecnología y proteja los derechos de protección de datos y los aspectos éticos asociados.

Respecto a la Protección de los y las Menores en el mundo online, se destacó la vulnerabilidad de los y las menores en el entorno digital, siendo necesario regular el acceso y uso de los y las menores a los servicios on-line, acompañado de programas adecuados de formación y concienciación.

Finalmente, respecto al tratamiento de neuroderechos y las neurotecnologías, se señaló la importancia que los desarrollos de las neurotecnologías están consiguiendo en la actualidad, así como los riesgos e impacto que dichos desarrollos representan para el derecho fundamental a la protección de datos. Se advirtió sobre el impacto potencial en la democracia y la esencia humana y se resaltó la importancia de los neuroderechos para proteger la privacidad y la autonomía frente a la manipulación y comercialización de los datos cerebrales.

8.2.5 Actualización página web RIPD

Durante la celebración del Encuentro Iberoamericano celebrado en el mes de mayo en Cartagena de Indias (Colombia), se presentó la actualización del sitio web de la RIPD, cuya puesta en producción se produjo en el mes de octubre.

Entre las implementaciones conseguidas durante 2024, destacan la actualización del gestor de contenidos de Drupal 8 a Drupal 10, mayor seguridad y flexibilidad en el diseño de contenidos; un cumplimiento de los estándares de accesibilidad; una mejora de la visualización del portal en móviles y otros dispositivos; la implementación de una serie de medidas encaminadas a la mejora del posicionamiento de la página en buscadores; la puesta en marcha de nuevas funcionalidades, como el buscador en Inglés y la activación de un Repositorio RIPD, con una estructura que diferencia documentos y herramientas y permite el diseño de carpetas compartidas para los distintos grupos de trabajo.

8.2.6 Alianza Digital EU_LAC. Gobernanza de Datos

En materia de Gobernanza de Datos, la Alianza Digital EU_LAC permitirá colaboraciones en Diálogos de Alto Nivel y la coordinación de los países miembros de la RIPD.

8.2.7 Colaboración con Red Asia-Pacífico de Protección de Datos (APPA)

La colaboración entre ambas redes se ha traducido en la elaboración de la guía sobre Cláusulas Contractuales Modelo (CCM ASEAN/RIPD) para facilitar las transferencias internacionales de datos entre ambas regiones. Esta guía busca establecer los principales aspectos que deben tenerse en cuenta cuando se realizan transferencias internacionales de datos personales (en adelante, TIDP) mediante el uso de cláusulas contractuales modelo (en adelante CCM) además presenta algunas orientaciones para que sean tenidas en cuenta por quienes deben realizar TIDP a jurisdicciones no adecuadas desde los países miembros de la RIPD.

8.2.8 Visitas Internacionales

Entre las visitas internacionales destacaron las realizada por la Secretaría de Derechos Digitales de Brasil, la de la autoridad chilena del Consejo Para La Transparencia (CPLT) y la del Instituto de Acceso a la Información Pública de Honduras (IAIP).

8.2.9 Participación en eventos internacionales

Respecto a la participación de la Agencia en eventos internacionales, cabe citar la presencia de representantes de la AEPD en el Privacy Symposium de Venecia; en el Children's Privacy and Safety in the World of Generative AI; en el Neurodata and Neurorights; en el I Congreso Internacional de Datos Personales celebrado en México; en el 1st inter-network meeting of data protection authorities, celebrado en Marruecos; la presencia virtual en el Webinar organizado por la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT); en el 9º aniversario de la CNPD de Cabo Verde y en el XI Congreso Internacional de Datos celebrado en Colombia.

8.2.10 Reuniones

Entre las reuniones en las que han participado representantes de la División de Relaciones Internacionales , tanto a nivel continental como fuera de Europa, destacan las celebradas con representantes de la OCDE; la UNESCO; la SEGIB; el ISMS Forum; con la Superintendencia de Protección de Datos de Ecuador; con representantes del PNUD (ONU); la AECID; con el Foro Sociedad Civil, la autoridad argentina (AAIP); la autoridad uruguaya AGESIC; el INAI de México; la autoridad de Andorra (APDA); la Agencia Brasileña (ANPD); la autoridad de Honduras (IAIP); con la FIIAP; la Alianza Digital UE-LAC; con PACCTO 2.0 y con Cuba Digital.

8.3 Supervisión de los Sistemas IT de Cooperación Policial y Judicial del Espacio de Libertad, Seguridad y Justicia - Nuevo Comité de Supervisión Coordinada

8.3.1 Comité de Supervisión Coordinada (CSC)

La AEPD participo durante 2024 en las 6 reuniones del Comité de Supervisión Coordinada. El CSC está formado por representantes de las autoridades nacionales de protección de datos de los países de la UE, más Islandia, Liechtenstein, Noruega y Suiza, y el Supervisor Europeo de Protección de Datos (SEPD). Fue creado en diciembre de 2019 para garantizar la supervisión coordinada de los sistemas informáticos de la UE a gran escala y de los órganos, oficinas y agencias pertinentes de la UE, de conformidad con el artículo 62 del Reglamento (UE) 2018/1725.

En marzo de 2023, el Sistema de Información de Schengen (SIS) pasó a ser competencia del CSC. En la actualidad, los sistemas informáticos, **órganos y organismos de la UE que entran en el ámbito de aplicación del CSC** son los siguientes:

- Sistema de Información del Mercado Interior (IMI)
- Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust)
- Agencia de Cooperación Policial de la Unión Europea (Europol)
- Sistema de Información de Schengen (SIS)
- Sistema de Información de Visados (VIS)

El CSC también ofrece un foro para la cooperación en el contexto de la Fiscalía Europea (EPPO).
Está previsto que **otros sistemas informáticos, organismos, oficinas y agencias de la UE entren en el ámbito de aplicación del CSC** en un futuro próximo. Se trata de los siguientes:

- Sistema de Entrada/Salida (EES)
- Sistema Europeo de Información y Autorización de Viajes (ETIAS)
- Sistema Europeo de Información de Antecedentes Penales de los no nacionales de la UE (ECRIS-TCN)
- Base de Datos Europea de Impresiones Dactilares de Asilo (EURODAC)
- Grupo de Supervisión Coordinada CIS (Custom Information System)
- Prüm II

De acuerdo con su programa de trabajo bianual, el CSC llevó a cabo sus actividades durante el periodo comprendido entre julio de 2022 y diciembre de julio de 2024 en torno a los cuatro **ejes principales** siguientes:

1. Promover y facilitar el ejercicio de los derechos de los interesados.
2. Examinar las dificultades de interpretación o aplicación de la legislación nacional y de la UE.
3. Intercambiar información y realizar auditorías conjuntas o inspecciones coordinadas.
4. Preparar la supervisión coordinada de los sistemas informáticos, organismos, oficinas y agencias de la UE que está previsto que entren en el ámbito de aplicación del CSC.

En abril de 2023, el CSC revisó, adoptó y publicó la siguiente guía elaborada por el SCG del SIS II: "*The Schengen Information System - a guide for exercising data subjects' rights: the right of access, rectification and erasure*"

Posteriormente, en julio de 2023 el CSC publicó la siguiente guía relativa a Europol: *Europol's information systems - a guide for exercising data subjects' rights: the right of access, rectification, erasure and restriction*'. Asimismo, en ese mismo

año, el CSC emprendió una actividad coordinada sobre Europol en relación con la transmisión por los Estados miembros de datos sobre menores sospechosos. Actualmente, está recopilando las conclusiones clave para redactar un informe conjunto sobre el ejercicio.

8.3.2 Grupo de Supervisión Coordinada CIS (Custom Information System)

Durante el año 2024, la AEPD ha participado en las reuniones anuales del CIS. El Grupo de Supervisión Coordinada se creó para almacenar información sobre mercancías, medios de transporte, personas y empresas, y dinero en efectivo, retenidos, incautados o confiscados, con el fin de ayudar a prevenir, investigar y perseguir las acciones contrarias a la legislación aduanera y agraria o las infracciones graves de la legislación nacional. El fichero FIDE es una base de datos conexa que almacena información sobre las personas físicas y jurídicas investigadas por infracción de la legislación aduanera. Una característica especial del CIS y de FIDE es que se basan en un doble fundamento jurídico: Reglamento (CE) nº515/97 del Consejo, de 13 de marzo de 1997, relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y a la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las reglamentaciones aduanera y agraria, y la Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros.

En sus últimas reuniones el CIS se ha centrado principalmente, en la evaluación del citad Reglamento (CE) nº 515/97, y en cuestiones relativas a la formación en materia de protección de datos del personal con acceso al Grupo de Coordinación de la Supervisión.

8.3.3 Grupo de Coordinación de la Supervisión de Eurodac (GCS) (sistema de información huellas dactilares)

La AEPD participo durante 2024 en las reuniones anuales del GCS Eurodac en el Comité Europeo de Protección de Datos. El objetivo principal de las reuniones citadas es debatir problemas comunes relacionados con la supervisión y encontrar soluciones o enfoques comunes siempre que sea posible. En la práctica, estas reuniones se celebran al menos dos veces al año. También se invita a la Comisión y a eu-LISA a participar a fin de informar al Grupo sobre las novedades relativas a Eurodac.

El 14 de mayo de 2024 se adoptó el Reglamento (UE) 2024/1358 del Parlamento europeo y del Consejo, sobre la creación del sistema «Eurodac» para la comparación de datos biométricos a efectos de la aplicación efectiva de los Reglamentos (UE) 2024/1351 y (UE) 2024/1350 del Parlamento Europeo y del Consejo y de la Directiva 2001/55/CE del Consejo y de la identificación de nacionales de terceros países y apátridas en situación irregular, y sobre las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 del Parlamento Europeo y del Consejo y se deroga el Reglamento (UE) 603/2013 del Parlamento Europeo y del Consejo.

El citado Reglamento se publicó en el Diario Oficial el 22 de mayo de 2024, y de conformidad con lo dispuesto en el Artículo 63, apartado 2, será aplicable a partir del 12 de junio de 2026. No obstante, conforme a lo indicado en el párrafo segundo del precepto anterior, el Artículo 26 de dicho Reglamento, relativo a la recopilación y transmisión de datos biométricos de nacionales de terceros países o apátridas registrados como beneficiarios de protección temporal, se aplicará a partir del 12 de junio de 2029.

En la última reunión del GCS Eurodac de fecha 9 de diciembre de 2024, la presidenta del Grupo informó a los miembros sobre la necesidad de un nuevo Programa de Trabajo para los próximos dos años (2025-2027).

8.3.4 Participación de la AEPD en otros foros internacionales

8.3.4.1. Consejo de Europa

Comité Consultivo y Mesa de la Convención 108+ del Consejo de Europa

Durante 2024 la Agencia Española de Protección de Datos participó en las dos reuniones ordinarias del Comité Consultivo en formación de Plenario y en las dos reuniones en formación de Mesa.

En noviembre de 2024 se produjo la renovación de la Mesa, órgano de dirección de los trabajos del Comité Consultivo. La Agencia ha dejado de formar parte de la Mesa citada, al no haber sido elegido el miembro de la delegación española que había sido seleccionado con anterioridad en el año 2022. Dado que la elección de los miembros es realizada a título personal, la Agencia sigue contando con un miembro en el Comité con representación en Plenario.

El "Convenio 108" fue el primer instrumento internacional jurídicamente vinculante creado en todo el mundo para proteger la privacidad en la era digital. Hasta la fecha 55 Estados han ratificado el tratado, incluidos los 46 Estados miembros del Consejo de Europa, así como Argentina, Cabo Verde, Marruecos, Mauricio, México, Senegal, Túnez y Uruguay. En 2018 se abrió a la firma un Protocolo que moderniza el "Convenio 108" (Convenio 108+) y tiene en cuenta los nuevos retos para la protección de datos personales surgidos desde 1981.

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 2024, un total de 46 Estados parte han firmado la convención, de los cuales 31 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 2023-24:

- Módulo segundo de las Cláusulas Contractuales Estándar del Consejo de Europa para transferencias internacionales de datos personales.
- Recomendaciones sobre protección de datos en los tratamientos de datos personales para la lucha contra el lavado de dinero, la falsificación y la financiación del terrorismo.
- Aprobación de la resolución de la Mesa de la convención para comenzar los trabajos sobre las recomendaciones en materia de protección de datos personales en el contexto de las neurociencias.

Comité de Inteligencia Artificial

Durante 2024 la Agencia Española de Protección de Datos participó en las cuatro reuniones ordinarias del Comité de Inteligencia Artificial (CAI) en formación de Plenario.

En fecha 17 de mayo de 2024, durante la reunión ministerial anual del Comité de Ministros del Consejo de Europa, celebrada en Estrasburgo, fue adoptado el **Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho**. Posteriormente, en fecha 5 de septiembre de 2024, el Convenio Marco citado fue firmado en Vilna (Lituania) por Andorra, Georgia, Islandia, Noruega, la República de Moldavia, San Marino, Reino Unido, Israel, Estados Unidos de América y la Unión Europea.

El Convenio Marco es el resultado de dos años de trabajo de un órgano intergubernamental, el Comité sobre Inteligencia Artificial, que reunió para redactar el tratado a los 46 Estados miembros del Consejo de Europa, la Unión Europea y 11 Estados no miembros (Argentina, Australia, Canadá, Costa Rica, Estados Unidos, Israel, Japón, México, Perú, la Santa Sede y Uruguay), así como a representantes del sector privado, la sociedad civil y el mundo académico, que participaron como observadores. Es el primer tratado internacional jurídicamente vinculante destinado a garantizar el respeto de los derechos humanos, del Estado de derecho y las normas jurídicas democráticas en el uso de los sistemas de inteligencia artificial (IA). El tratado, que también está abierto a países no europeos, establece un marco jurídico que abarca todo el ciclo de vida de los sistemas de IA y que se ocupa de los riesgos que pueden plantear, a la vez que promueve la innovación responsable.

Asimismo, durante la 12ª reunión plenaria, celebrada en Estrasburgo del 26 al 28 de noviembre, a la que asistió la AEPD, el Comité de Inteligencia Artificial adoptó la metodología HUDERIA, una nueva herramienta del Consejo de Europa que aporta directrices y un enfoque estructurado para llevar a cabo evaluaciones de riesgo e impacto de los sistemas de Inteligencia Artificial (IA). La **metodología HUDERIA** está específicamente diseñada para proteger y promover los derechos humanos, la democracia y el Estado de derecho y puede ser utilizada tanto por agentes públicos como privados.

En el año 2025 la metodología citada se complementará con el Modelo HUDERIA, que proporcionará materiales y recursos de apoyo, incluidas herramientas flexibles y recomendaciones ampliables.

8.3.4.2 Asamblea Global de Privacidad (GPA)

La 46ª edición de la Reunión Anual de la Asamblea Global de Privacidad tuvo lugar este año en Jersey del 28 de octubre al 1 de noviembre. Se aprobaron las siguientes resoluciones:

- Resolución por la que se respalda y fomenta el uso de mecanismos de certificación de la protección de datos.
- Resolución sobre los principios relativos al tratamiento de la información personal en neurociencia y neurotecnología.
- Resolución sobre la libre circulación de datos con confianza y una regulación eficaz de los flujos mundiales de datos.
- Resolución sobre las normas y procedimientos del ACP.

Todos estos documentos son accesibles en el siguiente **enlace**.

8.3.4.3 Grupo Internacional de Trabajo sobre Protección de Datos en Tecnología – Grupo de Berlín

El Grupo Internacional de Trabajo sobre Protección de Datos en Tecnología (IWGDPT por sus siglas en inglés), también denominado “Grupo de Berlín”, centra su atención en las tendencias y la evolución del sector tecnológico, como el "Big Data", el "Internet de las cosas o IoT" o la inteligencia artificial. Para ello, el grupo elabora recomendaciones y directrices para utilizar estas tecnologías de forma acorde con los requisitos de protección de datos.

En su trabajo conjunto, el Grupo de Berlín se beneficia de su composición heterogénea y transnacional, con participantes procedentes de autoridades supervisoras de la protección de datos, agencias gubernamentales, organizaciones internacionales y organizaciones no gubernamentales, así como de la investigación y el mundo académico. La AEPD aprecia especialmente el intercambio de opiniones y la cooperación con colegas internacionales para lograr las recomendaciones más completas y favorables a la protección de datos sobre nuevas tecnologías para un público internacional como es el público objetivo del Grupo de Berlín. Se reúne dos veces al año en distintas partes del mundo. Las reuniones del año 2024 tuvieron lugar en Oslo (Noruega) y en Bruselas (Bélgica).

Durante el año 2024 **el Grupo de Berlín aprobó y publicó** los siguientes documentos:

- Documento de trabajo sobre grandes modelos lingüísticos (LLM)
- Documento de trabajo sobre la puesta en común de datos
- Declaración conjunta sobre la 73ª reunión del Grupo IWGDPT de Berlín
- Documento de trabajo sobre la moneda digital de los bancos centrales (CBDC)
- Documento de trabajo sobre la tecnología de reconocimiento facial

Estos documentos se encuentran accesibles en el siguiente **enlace**.

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 Presidencia de la Agencia que, en caso de no atención al ejercicio de derechos y de posible vulneración de la normativa, analiza los indicios, realiza las actuaciones de investigación oportunas y, cuando procede, instruye los procedimientos sancionadores, de apercibimiento o de ejercicio de derechos, para proponer a la Presidencia la adopción de la resolución que corresponda.

Las reclamaciones pueden recibirse directamente en la Agencia, que es la situación más frecuente, aunque también pueden llegar a través de alguna de las Autoridades Autonómicas o de alguna Autoridad de Control de uno 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.

Como consecuencia de las reclamaciones para alcanzar una mejor y más concreta determinación de las conductas o hechos que puedan infringir la normativa de protección de datos se pueden realizar actuaciones previas de investigación. No obstante, estas actuaciones también pueden ser determinadas por propia iniciativa de la Presidencia de la Agencia.

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 Presidencia acuerda iniciar una investigación de oficio e instar a la SGID para que comience las actuaciones previas de investigación tendentes a acreditar los hechos.

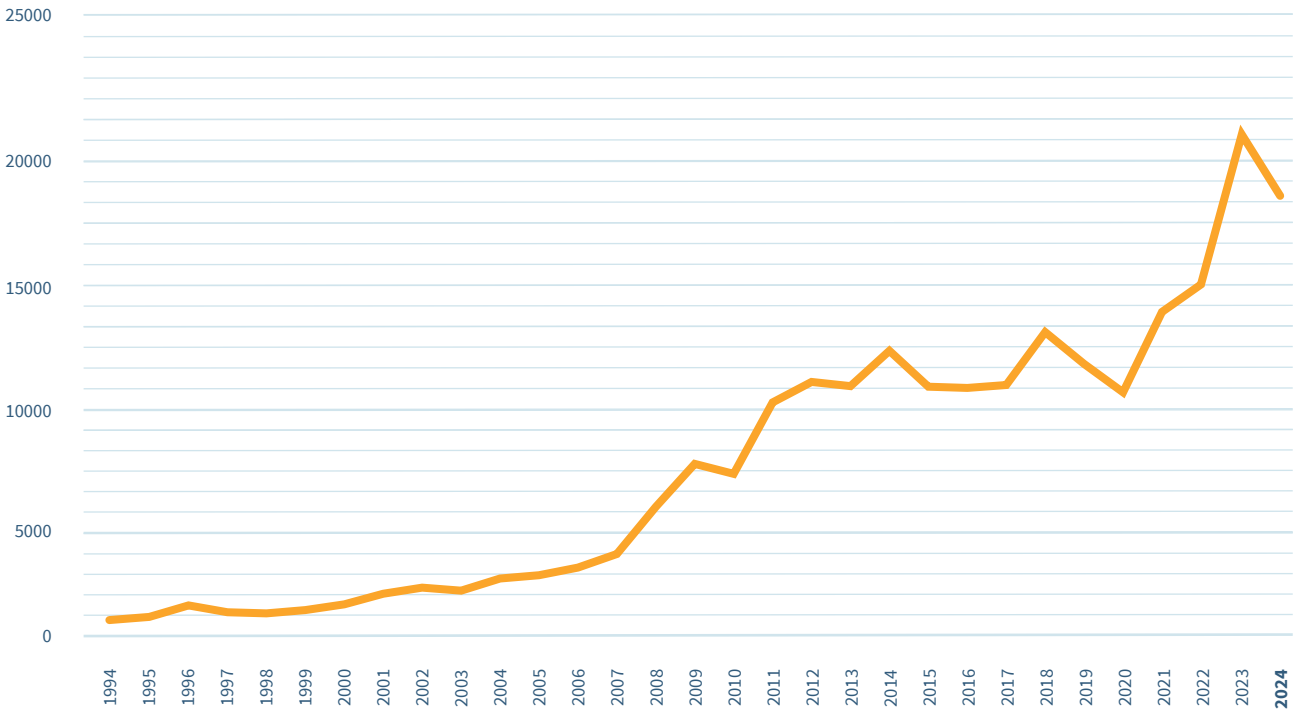
La siguiente tabla muestra estos datos y su comparación con los del ejercicio anterior:

Entradas de nuevos casos a la Subdirección General de Inspección de Datos					
Tipo de entrada	**2022**	**2023**	**2024**	**% relativo**	**Δ% anual**
Reclamaciones* presentadas ante la AEPD	15.128	21.590	18.855	96%	-13%
Casos transfronterizos procedentes de otras AC del EEE	651	708	825	4%	17%
Propia iniciativa de la AEPD (inc. brechas)	43	50	42	0%	-16%
TOTAL	**15.822**	**22.348**	**19.722**	**100%**	**-12%**

** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

La tendencia alcista en cuanto al número de entradas recibidas que se ha producido en los últimos años que presentaba una curva con una pendiente muy elevada se ha visto frenada durante el pasado 2024. No obstante, el número de reclamaciones recibidas este año ha sido un 25% superior a las recibidas durante el año 2022 y un 36% superior a las recibidas durante el año 2021, suponiendo el **segundo número de reclamaciones más alto de la historia de este organismo**, solo por detrás del récord del año 2023.

Reclamaciones presentadas en la AEPD



Este descenso tiene su explicación principal en la implantación de un buzón para la recepción de reclamaciones ("buzón guiado") que guía y orienta a los ciudadanos para facilitarles la información necesaria sobre las circunstancias necesarias y la documentación mínima a aportar para que su solicitud pueda ser atendida con garantías. Esta información se expresa de forma sencilla, por medio de preguntas de sí/no, que permiten al ciudadano conocer si su conflicto puede ser resuelto por la Agencia por estar en su ámbito competencial, y si dispone de la información y los indicios necesarios para que prospere. Durante 2024, este buzón se fue poniendo en funcionamiento en las principales categorías de reclamaciones, como son las de publicidad, videovigilancia o las reclamaciones sobre ejercicios de derechos. De esta forma, cuando un ciudadano quiere presentar una reclamación de alguna de las categorías mencionadas va siendo guiado por la aplicación antes de registrarla. En el caso de publicidad, que fue el primer buzón implantado y que ha estado en funcionamiento durante todo 2024, el descenso de reclamaciones presentadas ha sido notable como se observará en el apartado de clasificaciones, reduciendo asimismo el porcentaje de inadmisión de las reclamaciones efectivamente presentadas y facilitando a los ciudadanos la información que deben presentar para que su reclamación pueda prosperar y pueda ser analizada por la AEPD. Este aspecto es importante porque además no requiere a los ciudadanos que aporten información adicional para que la AEPD pueda evaluar su caso, sino que siguiendo las instrucciones que se marcan la información facilitada sería la necesaria.

No se rompe la tendencia alcista en los casos transfronterizos recibidos en la Agencia: en este año 2024 se han recibido un 17% más de casos que en el año 2023 y un 27% más que en el 2022. A pesar de ser una parte menor de la entrada, solo un 4% de las entradas que inician actuaciones, este tipo de reclamaciones son bastante más costosas tanto en tiempo como en esfuerzo del personal de la Agencia dado que existe la necesidad de llegar a un consenso con otras autoridades del EEE, de comprender la normativa local, según el caso y de relacionarse en otro idioma.

En 2024 la tasa de reclamaciones resueltas frente a reclamaciones recibidas ha aumentado ligeramente a un 96% frente el 94% del año anterior, estabilizando esta ratio. A las reclamaciones recibidas hay que sumarle aquellas que quedaron pendientes del año anterior, el 2023. A pesar de los esfuerzos realizados en los años previos, y también durante 2024, el número de reclamaciones pendientes al finalizar el año ha ido en aumento desde el año 2021. Se debe llamar la atención sobre la falta de aumento de personal en 2024, a pesar del ingente aumento en el número de reclamaciones que se ha experimentado desde 2021 que exige un aumento proporcionado y constante en los medios personales de la SGID. Esta carencia de personal unida a la mayor complejidad de las reclamaciones, que han ido cambiando de manera significativa hacia aspectos más tecnológicos que requieren un mayor nivel de conocimiento, es el origen de este aumento en las reclamaciones pendientes de finalizar.

Las reclamaciones resueltas en el año 2024 han descendido un 11% con respecto al año anterior; hay que destacar que también ha disminuido en ese porcentaje el número de escritos de entrada, como se ha visto en la tabla anterior. No obstante, el número de reclamaciones resueltas es un 20% más que las resueltas en el año 2022. La complejidad de los casos reclamados va en aumento, y se une a la efectividad del buzón guiado para que las reclamaciones que se reciban sean más consistentes y por tanto se tramiten en mayor medida con procedimientos más costosos en esfuerzo. Mientras que anteriormente un gran número de reclamaciones se resolvían con inadmisiones por falta de indicios suficientes de infracción en el ámbito competencial de la Agencia, el buzón guiado permite que el ciudadano esté mejor informado y presente reclamaciones más completas y mejor dirigidas, con indicios suficientes de infracción.

En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

Reclamaciones resueltas y pendientes				
Tasa de resolución de reclamaciones	**2022**	**2023**	**2024**	**Δ% anual**
Reclamaciones* resueltas en el año	14.937	20.391	18.132	-11%
Reclamaciones pendientes de resolver al finalizar el año	3.707	4.906	5.629	15%
Tasa de reclamaciones resueltas vs. recibidas en el año	99%	94%	96%	2%

** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

2. Resoluciones

Uno de los indicadores que muestran la actividad que se realiza desde la Subdirección General de Inspección de Datos es el número de resoluciones y actos finalizadores del expediente que se emiten. Las entradas reflejadas en el apartado anterior pueden dar lugar a diferentes actuaciones y procedimientos que finalizan con este tipo de actos definitivos. El número de entradas tramitadas no tiene que coincidir necesariamente con el número de actos firmados: 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.

Este año 2024, el porcentaje de inadmisiones en esta fase se ha visto reducido en casi 10 puntos porcentuales, situándose en el 60% en relación al número de resoluciones finalizadas en otras fases que se sitúa en el 40%. Esto está relacionado de manera directa con el buzón guiado y la calidad de las reclamaciones que llegan a esta primera fase. Así, se producen menos inadmisiones por falta de indicios con mayor satisfacción para los ciudadanos.

De esta manera se ve materializado el esfuerzo puesto por parte de la Agencia para que las reclamaciones recibidas sean de calidad, aportando la documentación mínima necesaria para poder ser admitidas, tal y como se especifica en Resolución de 29 de junio de 2023, de la Dirección de la Agencia Española de Protección de Datos, por la que se aprueban los modelos de presentación de reclamaciones, en los que se detalla la información que tienen que aportar los reclamantes para que su reclamación pueda surtir efectos.

La siguiente tabla muestra los datos referentes a estas finalizaciones en fase de análisis previo:

Finalizaciones del expediente en la fase de Análisis previo de la reclamación				
Tipo de resultado	**2023**	**2024**	**% relativo**	**Δ% anual**
Finalización del expediente tras el Análisis previo de la reclamación **	**13.791**	**10.515**	**60%**	**-24%**
Inadmisiones a trámite*	13.510	10.211	58%	-24%
Competencia de otras AC nacionales (CGPJ, AC auton.)*	281	304	2%	8%
Finalizaciones del expediente en otras fases **	**6.282**	**7.014**	**40%**	**12%**
TOTAL	**20.073**	**17.529**	**100%**	**-13%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*
*** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

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 y con un mayor agrado de los ciudadanos que ven resuelto su problema en un plazo muy breve.

La inclusión de la fase de traslado ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. En 2024, siguiendo la línea iniciada en el año 2023, de las reclamaciones que prosperaron tras el análisis previo de la reclamación y tras haber procedido al traslado de la reclamación, se resolvió finalizando el expediente en el 88% de los casos, dando así una respuesta más rápida a los reclamantes que la que se conseguía con la normativa anterior y solucionando de una manera más ágil su reclamación. El aumento del porcentaje de reclamaciones que se resuelven en fases tempranas (análisis previo de admisibilidad y traslado de la reclamación), ha conllevado la consecuente reducción en el número de actuaciones previas de investigación y de procedimientos. Esto permite a la SGID responder a la mayor complejidad de los tratamientos analizados con una adecuada distribución de los recursos disponibles, puesto que estas actuaciones posteriores requieren una importante dedicación de tiempo y personas.

Por su parte, la Agencia consideró la existencia de responsabilidades que debían ser depuradas en procedimiento sancionador o de apercibimiento en el 6% de los casos que pasaron la fase de análisis previo de admisibilidad. 2024 es el primer año completo en el que se han tramitado procedimientos de apercibimiento, incluidos en la LOPDGDD en el año 2023, de manera separada a los sancionadores. En la siguiente tabla se muestra la distribución completa de resoluciones y actos finalizadores según la fase en que se alcanza la finalización del caso:

Finalización de los expedientes en fases posteriores al análisis previo de la reclamación				
Tipo de resultado en fases posteriores al análisis previo	**2023**	**2024**	**% relativo**	**Δ% anual**
Finalización del expediente tras el Traslado de la reclamación*	**5.401**	**6.201**	**88%**	**15%**
Respuesta satisfactoria del responsable o encargado	3.475	2.581	37%	-26%
Ser plena competencia de otra AC del EEE	531	603	9%	14%
Actuar como autoridad interesada en el EEE (archivo provisional)	274	340	5%	24%
Otros motivos tras traslado**, ***	1.121	2.677	38%	139%
Finalización del expediente tras las actuaciones previas de investigación	**143**	**146**	**2%**	**2%**
Archivo de actuaciones previas de investigación	143	146	2%	2%
Finalización del expediente en el procedimiento de ejercicio de derechos	**246**	**253**	**4%**	**3%**
Resuelto en el procedimiento de ejercicio de derechos	246	253	4%	3%
Finalización del expediente en el procedimiento sancionador	**489**	**362**	**5%**	**-26%**
Resuelto en procedimiento sancionador – Multa	367	281	4%	-23%
Resuelto en procedimiento sancionador – Infracción de las AAPP	58	37	1%	-36%
Resuelto en procedimiento sancionador – Archivo	64	44	1%	-31%

Finalización de los expedientes en fases posteriores al análisis previo de la reclamación				
Tipo de resultado en fases posteriores al análisis previo	2023	2024	% relativo	Δ% anual
Finalización del expediente en el procedimiento de apercibimiento	**3**	**52**	**1%**	**1633%**
Resuelto en procedimiento de apercibimiento – Apercibimiento	3	44	1%	1367%
Resuelto en procedimiento de apercibimiento – Archivo	0	8	0%	-
TOTAL	**6.282**	**7.014**	**100%**	**12%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** Incluye el envío de información al responsable del tratamiento de sus obligaciones en relación con la infracción denunciada, la normativa a la que debe dar cumplimiento, y el recordatorio de que en caso de no ajustarse se podrá iniciar las actuaciones pertinentes.*

**** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

2.3 Tiempos medios de resolución

Se reflejan a continuación los tiempos medios, en días, hasta que se dicta resolución o acto finalizador del expediente. Debe tenerse en cuenta que las resoluciones que se realizan antes de la admisión a trámite son de inadmisión. 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.

Tiempo medio de finalización del expediente en la fase de análisis previo de la reclamación			
Tiempos medios de resolución en fase de Análisis (en días)	2023	2024	Δ% anual
Finalización del expediente en el Análisis previo de la reclamación*; **	32	26	-19%
TIEMPO MEDIO	**32**	**26**	**-19%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

Los tiempos de análisis previo de la reclamación descienden. Este descenso va ligado al volumen de las reclamaciones recibidas cuyo número superó la capacidad de los recursos dedicados en 2023 y que en 2024 se ha moderado. 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/archivo, tras el traslado al responsable y el análisis de la respuesta recibida. El tiempo medio es inferior a los tres meses que dispone la normativa para la admisión a trámite, y se ha reducido respecto al del año previo.

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 y de apercibimiento, son los transcurridos desde la fecha de admisión a trámite de la reclamación hasta que se firma la resolución.

Los tiempos medios de resolución de las actuaciones previas de investigación y de los procedimientos han aumentado, mostrando una vez más la mayor complejidad de los tratamientos de datos que se realizan y que deriva en una mayor dedicación por parte del personal en las investigaciones y procedimientos de la Agencia. También es resultado directo del aumento en los plazos de caducidad de las actuaciones previas de investigación y de los procedimientos sancionadores, que desde 2023 quedó fijado legalmente en 18 y 12 meses respectivamente (frente a los 12 y 9 meses marcados anteriormente, lo que supone un aumento del 15% y del 33% respectivamente), permitiendo un análisis más profundo de las causas determinantes en los expedientes más complejos.

A pesar de ello, el tiempo medio global de resolución se ha reducido en 8 días (un 7%) respecto al año 2023. Este valor también es inferior al de los años previos y se logra gracias al descenso del tiempo medio de las resoluciones en la fase de traslado, que representan una gran mayoría.

Tiempo medio de finalización del expediente según el procedimiento en que se resuelve, una vez pasada la fase de análisis previo de la reclamación

Tiempos medios de finalización del expediente según el procedimiento tras pasar la fase de análisis previo (en días)	2023	2024	Δ% anual
Finalización del expediente tras las actuaciones de traslado*; **	91	77	-15%
Finalización del expediente tras las actuaciones previas de investigación	269	299	11%
Finalización del expediente en el procedimiento de ejercicio de derechos	110	125	14%
Finalización del expediente en el procedimiento sancionador	292	420	44%
Finalización del expediente en el procedimiento de apercibimiento	191	365	91%
TIEMPO MEDIO	**111**	**103**	**-7%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

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, pero que no necesariamente resuelven el expediente, incluye actuaciones intermedias y por tanto que representa el trabajo total realizado en la SGID (frente al apartado anterior, que solo mostraba los actos finalizadores del expediente). Un ejemplo de ello sería unas actuaciones previas de investigación que dan 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 generan una resolución que pone 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 del año.

Se puede observar una reducción de reclamaciones analizadas como consecuencia de la reducción de reclamaciones recibidas en la Agencia. A pesar de la reducción, este número es todavía muy superior, un 30%, a las reclamaciones analizadas durante el año 2022.

Por el contrario, el número de resoluciones en la fase de traslado de la reclamación al responsable o encargado del tratamiento sigue en aumento en línea con el año anterior. Esto muestra como el mayor impacto de la reducción de reclamaciones recibidas está en la primera fase de análisis previo. Y viene a corroborar que las reclamaciones presentan una mayor calidad en cuanto a la información y documentación aportada.

Los procedimientos sancionadores muestran un descenso por un motivo evidente, este 2024 incluye los procedimientos de apercibimiento que resuelven cierto tipo de infracciones, cuyo trámite se encuentra ahora separado de los procedimientos sancionadores después de la modificación legal en la LOPDGDD de 2023. También es consecuencia del aumento de resoluciones en fases previas de traslado de la reclamación.

El descenso de los recursos de reposición tramitados es acorde con la reducción del número de resoluciones de procedimientos.

Actuaciones realizadas			
Número de actuaciones finalizadas según la fase del procedimiento	2023	2024	Δ% anual
Reclamaciones analizadas*	21.590	18.986	-12%
Actuaciones de traslado*	6.281	7.146	14%
Actuaciones previas de investigación	316	311	-2%
Procedimientos de ejercicio de derechos	246	253	3%
Procedimientos sancionadores	490	362	-26%
Procedimientos de apercibimiento	3	52	1633%
Recursos de reposición	940	854	-9%
TOTAL	**29.866**	**27.964**	**-6%**

** 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. Así, por ejemplo, el tiempo medio que transcurre desde que se recibe una reclamación hasta que se completa su análisis previo de admisibilidad (con independencia de que el resultado de ese análisis sea la finalización en esa fase o su continuación) es de 24 días. La misma causa que se expuso al describir el aumento de los tiempos medios de resolución aplica naturalmente a cada una de las fases del procedimiento.

Tiempos medios de tramitación en cada fase del procedimiento			
Tiempos medios de actuaciones realizadas en la gestión de la reclamación según la fase del procedimiento (en días)	2023	2024	Δ% anual
Reclamaciones analizadas*, **	31	24	-22%
Actuaciones de traslado*, **	56	53	-6%
Actuaciones previas de investigación	206	246	19%
Procedimientos de ejercicio de derechos	84	93	11%
Procedimientos sancionadores	130	180	39%
Procedimientos de apercibimiento	31	111	253%
Recursos de reposición	106	76	-28%
TIEMPO MEDIO	**43**	**39**	**-10%**

** Incluye reclamaciones relacionadas con el ejercicio de derechos.*

*** Incluye toda reclamación por infracción de la normativa, con independencia de que los datos personales conciernan al reclamante.*

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.

En la tabla siguiente se informa, para el año 2024, de 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 la de declaración de infracción.

Administraciones Públicas sancionadas por incumplimiento de requerimientos y medidas correctivas

Investigado	Tipo entidad investigada	Artículo infringido	Artículo de tipificación	Resolución
Ayuntamiento de Ávila	Administración Local	RGPD 58.2	83.6	https://www.aepd.es/documento/ps-00449-2023.pdf
Ayuntamiento de San Cristóbal de La Laguna	Administración Local	RGPD 58.1	83.5	https://www.aepd.es/documento/ps-00064-2024.pdf
Ayuntamiento de San Cristóbal de La Laguna	Administración Local	RGPD 58.1	83.5	https://www.aepd.es/documento/ps-00131-2024.pdf
Ayuntamiento de Santiago de Compostela	Administración Local	RGPD 58.1	83.5	https://www.aepd.es/documento/ps-00428-2024.pdf

5. Brechas de datos personales

En caso de brechas de datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 del RGPD. Cuando como consecuencia de dicha notificación se aprecie la necesidad determinar una posible vulneración de la normativa de protección de datos, la Presidencia puede ordenar a la SGID realizar las oportunas investigaciones previas de oficio. Asimismo, los ciudadanos pueden reclamar a la Agencia cualquier infracción relacionada con una brecha de datos personales en la que se hayan visto afectados. En uno u otro caso, la Agencia ha realizado actuaciones previas de investigación con vistas a determinar la posible infracción y el responsable de la misma, que finalmente ha derivado en importantes procedimientos realizados durante 2024.

Tipo de actuación realizada	2023	2024	Δ% anual
Actuaciones previas de investigación	31	36	16%
Procedimientos sancionadores o de apercibimiento	25	30	20%
Importe total de multas impuestas	**13.180.800 €**	**13.179.600 €**	**0%**

Las infracciones determinadas más comunes en estos procedimientos incluyen la pérdida de confidencialidad (art. 5.1.f RGPD), la falta de observación de la protección de datos desde el diseño y por defecto (art. 25 RGPD), la falta de medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32 RGPD) o la falta de notificación de la brecha a la autoridad de control (art. 33 RGPD) o a los afectados cuando sea probable que entrañe un alto riesgo para sus derechos y libertades (art. 34 RGPD). Para determinar estas infracciones se hace necesario el desarrollo de actuaciones de investigación amplias y de procedimientos complejos. Entre los procedimientos más relevantes resueltos en 2024 relacionados con brechas de datos personales se pueden citar los siguientes, que culminaron con la imposición de algunas de las multas más altas del año:

Responsable	Infracción	Multa	Resolución
GENERALI ESPAÑA, S. A. DE SEGUROS Y REASEGUROS	Art. 5.1.f, 32, 35, 25 RGPD	4.000.000€	https://www.aepd.es/documento/ps-00453-2023.pdf
I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U.	Art. 25, 32 y 5.1.f RGPD	3.500.000€	https://www.aepd.es/documento/ps-00145-2023.pdf
IBERDROLA, S.A.	Art. 32 y 5.1.f RGPD	3.000.000€	https://www.aepd.es/documento/ps-00221-2023.pdf
TELEFÓNICA DE ESPAÑA, S.A.U.	Art. 32 y 5.1.f RGPD	1.300.000€	https://www.aepd.es/documento/ps-00291-2023.pdf

6. Recursos

Los recursos interpuestos frente a resoluciones de los procedimientos de la SGID se muestran a continuación, según hayan sido de reposición, extraordinarios de revisión, o contencioso-administrativos.

Recursos recibidos			
Tipo de recurso	**2023**	**2024**	**Δ% anual**
Recursos de reposición	952	872	-8%
Solicitudes o recursos extraordinarios de revisión	16	21	31%
Recursos contencioso-administrativos	128	145	13%
TOTAL	**1.096**	**1.038**	**-5%**

Los recursos de reposición y revisión resueltos anualmente por la AEPD se muestran en la siguiente tabla. A pesar de la reducción de recursos resueltos con respecto al año anterior, estos siguen siendo superiores a los del año 2022. Esta reducción va asociada a la reducción de la presentación de reclamaciones de este año 2024.

Recursos resueltos			
Tipo de recurso	**2023**	**2024**	**Δ% anual**
Recursos de reposición	940	854	-9%
Recursos extraordinarios de revisión	18	21	17%
TOTAL	**958**	**875**	**-9%**

7. Clasificaciones

7.1 Reclamaciones planteadas con mayor frecuencia

Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2023, que suponen algo más del 80% del total de reclamaciones recibidas en el año:

Reclamaciones más frecuentes				
Reclamaciones planteadas con mayor frecuencia	2023	2024	% relativo	Δ% anual
TOP 10	**18.211**	**15.558**	**83%**	**-15%**
Videovigilancia	2.865	3.411	18%	19%
Servicios de Internet	2.909	3.141	17%	8%
Comercio, transporte y hostelería	1.529	1.633	9%	7%
Publicidad	4.947	1.297	7%	-74%
Entidades financieras/acreedoras	1.385	1.219	6%	-12%
Ficheros de Morosidad	1.267	1.096	6%	-13%
Asuntos laborales	718	1.070	6%	49%
Administración pública	808	979	5%	21%
Sanidad	802	876	5%	9%
Reclamación de Deudas	981	836	4%	-15%
Otros	**3.379**	**3.297**	**17%**	**-2%**
TOTAL	**21.590**	**18.855**	**100%**	**-13%**

El cambio más notable en la clasificación de este año es la drástica reducción en el número de reclamaciones recibidas con relación a la recepción de publicidad no deseada. Esto es fruto de la implantación del buzón guiado, cuyo origen estuvo precisamente en esta tipología de reclamaciones dado su elevado número (el 20% de todas las reclamaciones recibidas durante el 2023). En este 2024 siguen presentes entre las más frecuentes, pero de manera más limitada, representando el 7% del total.

Sin embargo y a pesar de haber implantado el buzón guiado también en el área de videovigilancia, las reclamaciones de esta materia constituyen el 18% de las reclamaciones recibidas y ha aumentado en un 19% frente a los datos del año anterior. La facilidad para instalar cámaras de videovigilancia y su bajo coste ha hecho prosperar este tipo de instalaciones, que en muchos casos se instalan sin unas garantías adecuadas en relación a la normativa de protección de datos.

7.2 Áreas más frecuentes en procedimientos sancionadores y de apercibimiento

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores y de apercibimiento finalizados en 2024, que representan casi el 80% del total de estos procedimientos resueltos en el año:

Procedimientos sancionadores más frecuentes				
Grupo de actividad	2023	2024	% relativo	Δ% anual
TOP 10	**427**	**329**	**79%**	**-23%**
Videovigilancia	164	84	20%	-49%
Servicios de Internet	71	78	19%	10%
Publicidad	41	33	8%	-20%
Comercio, transporte y hostelería	26	26	6%	0%
Asuntos laborales	18	23	6%	28%
Contratación fraudulenta	26	22	5%	-15%
Administración pública	31	21	5%	-32%
Telecomunicaciones	27	15	4%	-44%
Quiebras de seguridad	14	14	3%	0%
Derechos protección de datos	9	13	3%	44%
Otros	**66**	**85**	**21%**	**29%**
TOTAL	**493**	**414**	**100%**	**-16%**

Un año más siguen destacando los procedimientos de videovigilancia, aunque han sufrido un descenso considerable motivado en parte por la resolución temprana de los casos de videovigilancia en fase de análisis y traslado de la reclamación. El segundo motivo destacado son los relacionados con los servicios de Internet.

8. 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.

8.1 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.

Casos transfronterizos participados			
Papel de la AEPD	**2023**	**2024**	**Δ% anual**
Nuevos casos liderados como autoridad principal	25	22	-12%
Nuevos casos en cooperación como autoridad interesada	301	348	16%
TOTAL	**326**	**370**	**13%**

De los casos en los que España ha actuado como autoridad principal, cabe destacar los siguientes procedimientos, por el importe de la multa impuesta:

Principales casos transfronterizos en los que la Agencia ha sido autoridad principal		
Responsable	**Infracción**	**Multa**
OK MOBILITY ESPAÑA, S.L.	Art. 5.1.e, 13 y 15 del RGPD	60.000 €
IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERADORA	Art. 15 del RGPD	40.000 €
GLOVOAPP23, S.A.	Art. 15 del RGPD	15.000 €

Como se puede observar, la mayoría de ellos se refieren a infracciones de derechos. Se puede leer más sobre estos y más casos transfronterizos participados como autoridad líder en el apartado “6.2 Reclamaciones y procedimientos más relevantes”.

En cuanto a los casos en los que la AEPD ha participado como autoridad interesada, dado su relevancia e importe de la multa impuesta, cabe destacar los siguientes casos:

Principales casos transfronterizos en los que la Agencia ha sido autoridad interesada		
Responsable	**Multa**	**Autoridad principal**
META PLATFORMS IRELAND LIMITED	91.000.000 EUR	Irlanda
LINKEDIN	310.000.000 EUR	Irlanda
AVAST	≈ 13,657.587 EUR*	República Checa
CONTEXTLOGIC	2.140.000 EUR	Países Bajos
UBER	290.000.000 EUR	Países Bajos
NUXE	100.000 EUR	Francia

** Sanción impuesta en coronas checas. Conversión a euros aproximada.*

La tramitación de estos procedimientos fue realizada por la autoridad de control del Estado miembro del Espacio Económico Europeo (EEE) en que se sitúa el establecimiento principal de cada responsable, en cooperación con la AEPD y otras autoridades interesadas. Las resoluciones han sido publicadas por la autoridad de ese país y se recogen en el repositorio del Comité Europeo de Protección de Datos.

8.2 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.

El número de casos procedentes de otras autoridades crece en un 17%, mientras que las solicitudes de asistencia lo hacen en un 26%. Esto refleja como cada vez es mayor la cooperación entre las autoridades de los diferentes países del EEE y cómo los tratamientos de datos cada vez tienen un ámbito mayor, pasando las fronteras de los países y afectando a ciudadanos a lo largo de más de un territorio.

Solicitudes y decisiones recibidas en procedimientos de cooperación			
Tipo de entrada	**2023**	**2024**	**Δ% anual**
Casos transfronterizos procedentes de otras AC	708	825	17%
Solicitudes de asistencia de otras AC	294	370	26%

Solicitudes y decisiones recibidas en procedimientos de cooperación			
Tipo de entrada	**2023**	**2024**	**Δ% anual**
Consultas de otras AC en procedimientos transfronterizos	51	47	-8%
Proyectos de decisión de casos en los que la AEPD participa*	99	101	2%
Operaciones conjuntas en las que la AEPD participa	0	0	0%
TOTAL	**1.152**	**1.343**	**17%**

** 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.*

8.3 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.

En línea con la tabla anterior, se puede ver como desde la Agencia se han emitido más solicitudes y casos con otras autoridades. Es notable el ascenso de casos transfronterizos compartidos, siendo un 66% superior al año anterior. También crecen las solicitudes de asistencia y las consultas a otras autoridades. Sin embargo, este año el número de proyectos de decisión emitidos en casos liderados por la AEPD ha sido más reducido.

Solicitudes y decisiones remitidas en procedimientos de cooperación			
Tipo de notificación	**2023**	**2024**	**Δ% anual**
Casos transfronterizos compartidos con otras AC	64	106	66%
Solicitudes de asistencia a otras AC	102	114	12%
Consultas a otras AC en procedimientos transfronterizos	10	11	10%
Proyectos de decisión de casos liderados por la AEPD*	48	19	-60%
Operaciones conjuntas en las que la AEPD participa	0	0	0%
TOTAL	**224**	**250**	**12%**

** 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.*

8.4 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).

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.
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.
Chap GPT	Grupo de trabajo creado para armonizar las decisiones de cada una de las Autoridades en relación a este asunto, al no existir, inicialmente un establecimiento principal en EEE y ser todas las autoridades, autoridades principales.

9. Multas

9.1 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:

Volumen de multas			
Evolución de las multas impuestas	**2023**	**2024**	**Δ% anual**
Número de multas	367	281	-23%
Importe total	29.817.410 €	35.592.200 €	19%

El número total de multas interpuestas es menor que en año 2023, pero el importe global de las mismas es casi un 20% superior, todo ello refleja una vez más la mayor complejidad de los tratamientos analizados, su mayor alcance, y por tanto mayor impacto de las infracciones.

Debe considerarse que el Comité Europeo de Protección de Datos ha elaborado unas **directrices** sobre el cálculo de multas para intentar que todas las autoridades sigan unos criterios armonizados en la imposición de multas.

Las multas superiores al millón de euros impuestas a personas jurídicas por resoluciones firmadas en 2024 y que han devenido firmes y ejecutivas son publicadas por la Agencia en el BOE, de conformidad con lo establecido por la LOPDGDD.

Volumen de multas			
Responsable	**Infracción**	**Multa**	**Resolución**
ENERGYA VM GESTIÓN DE ENERGÍA, S.L.	Art. 5.1.a y 5.2 RGPD	5.000.000€	https://www.aepd.es/documento/ps-00216-2023.pdf
GENERALI ESPAÑA, S. A. DE SEGUROS Y REASEGUROS	Art. 5.1.f, 32, 35, 25 RGPD	4.000.000€	https://www.aepd.es/documento/ps-00453-2023.pdf
CAIXABANK, S.A.	Art. 32 y 5.1.f RGPD	3.500.000€	https://www.aepd.es/documento/ps-00477-2023.pdf
I-DE REDES ELÉCTRICAS INTELIGENTES, S.A.U.	Art. 25, 32 y 5.1.f RGPD	3.500.000€	https://www.aepd.es/documento/ps-00145-2023.pdf

Volumen de multas			
IBERDROLA, S.A.	Art. 32 y 5.1.f RGPD	3.000.000€	https://www.aepd.es/documento/ps-00221-2023.pdf
TELEFÓNICA DE ESPAÑA, S.A.U.	Art. 32 y 5.1.f RGPD	1.300.000€	https://www.aepd.es/documento/ps-00291-2023.pdf
CAIXABANK, S.A.	Art. 6.1 RGPD	1.200.000€	https://www.aepd.es/documento/ps-00032-2024.pdf
ORANGE ESPAGNE, S.A.U.	Art. 6 y 25 RGPD	1.200.000€	https://www.aepd.es/documento/ps-00332-2023.pdf
BANCO BILBAO VIZCAYA ARGENTARIA, S.A.	Art. 32, 25, 6.1, y 32 RGPD	1.184.000€	https://www.aepd.es/documento/ps-00677-2022.pdf
LIGA NACIONAL DE FUTBOL PROFESIONAL	Art. 35 RGPD	1.000.000€	https://www.aepd.es/documento/ps-00484-2023.pdf

9.2 Áreas con mayor importe global de multas

La siguiente tabla desglosa las 5 áreas de actividad con mayor importe en sanciones en 2024, destacando los sectores relacionados con las multas más voluminosas detalladas en el apartado anterior:

Desglose de multas por temas				
Importe de multas en euros según el tema	**2023**	**2024**	**% relativo**	**Δ% anual**
Cinco temas con mayor importe total en 2024	**9.824.700€**	**27.453.080€**	**77%**	**179%**
Energía/Agua	115.500€	11.680.600€	33%	10013%
Entidades financieras/acreedoras	5.321.000€	5.356.900€	15%	1%
Servicios de Internet	1.058.700€	4.547.380€	13%	330%
Telecomunicaciones	1.942.000€	3.330.000€	9%	71%
Contratación fraudulenta	1.387.500€	2.538.200€	7%	83%
Otros	**19.992.710€**	**8.139.120€**	**23%**	**-59%**
TOTAL	**29.817.410€**	**35.592.200€**	**100%**	**19%**

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 que puede causar un daño irreparable a los afectados, 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.

Entradas recibidas por el Canal Prioritario			
Tipo de entrada	**2023**	**2024**	**Δ% anual**
Reclamaciones presentadas ante la AEPD	413	454	10%
Comunicaciones del canal de menores (14-18 años)	159	108	-32%
TOTAL	**572**	**562**	**-2%**

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 por el daño que puedan causar a las personas reclamantes, 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.

La siguiente tabla muestra las entradas que, después de dicho análisis, fueron canalizadas por el canal urgente.

Entradas tratadas por vía urgente			
Tipo de entrada	**2023**	**2024**	**Δ% anual**
Reclamaciones recibidas por el Canal Prioritario	29	40	38%
Reclamaciones recibidas por canales ordinarios	7	13	86%
Comunicaciones del canal de menores (14-18 años)	5	2	-60%
TOTAL	**41**	**55**	**34%**

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.

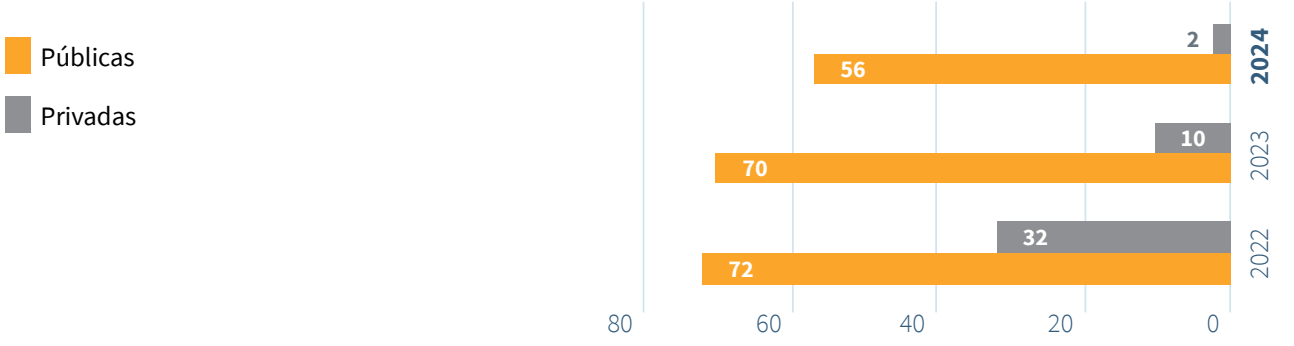
Intervenciones de retirada de contenidos			
Tipo de Actuación	**2023**	**2024**	**Δ% anual**
Intervenciones con carácter de urgencia para la retirada de contenidos	**36**	**62**	**72%**
Medidas cautelares adoptadas	26	33	27%
Solicitudes de retirada urgente enviadas	10	29	190%
Intervenciones que han resultado eficaces	**34**	**51**	**50%**
Medidas cautelares que han resultado eficaces	24	30	25%
Solicitudes de retirada urgente que han resultado eficaces	10	21	110%
Eficacia de las intervenciones para la retirada de contenidos	**94%**	**82%**	**-12%**
Medidas cautelares adoptadas	92%	91%	-1%
Solicitudes de retirada urgente enviadas	100%	72%	-28%

2. Gabinete Jurídico

Consultas

	Administraciones Públicas
AGE	48
CCAA	3
Entidades locales	1
Empresas públicas	0
Otros Organismos	4
TOTAL 1	**56**
	Consultas Privadas
Asociaciones y Fundaciones	0
Empresas	2
Particulares	0
Sindicatos	0
Otros	0
TOTAL 2	**2**
TOTAL	**58**

Evolución de consultas



Evolución de consultas por sectores (2023 - 2024)		
	2023	2024
Administraciones Públicas	61	**56**
Sanidad / Salud Pública	5	**7**
Telecomunicaciones	8	**3**
Asociaciones y fundaciones	1	**0**
Solvencia patrimonial / morosidad	1	**1**
Servicios financieros	1	**3**
Servicios mensajería	2	**0**
Seguros	2	**4**
Educación	2	**0**

Nota: Existen consultas que afectan a varias cuestiones y pueden ser clasificadas en más de un sector. Otras categorias estan 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.

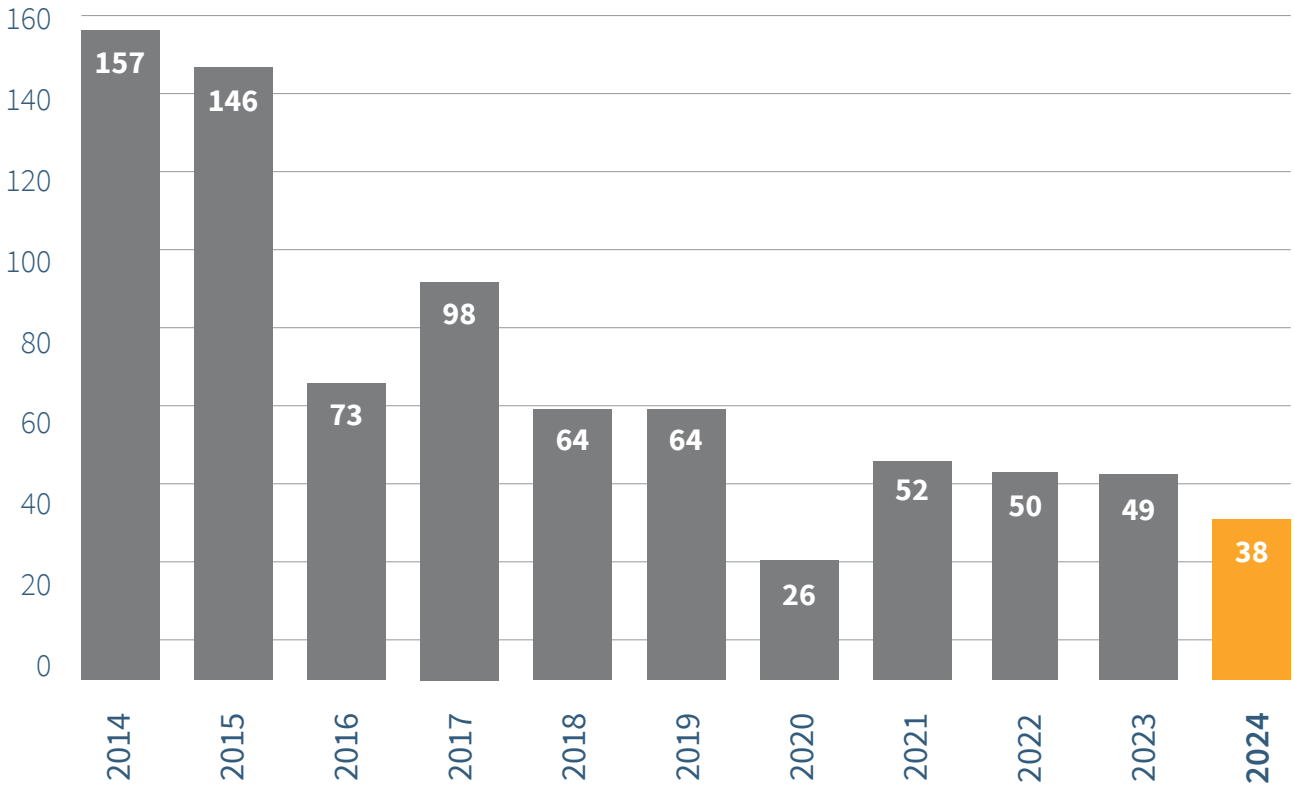
Evolución de consultas por materias (2023 - 2024)		
	2023	2024
Conceptos Generales*	49	**40**
Ámbito de Aplicación	1	**1**
Licitud	15	**6**
Derecho de Información y Transparencia	9	**0**
Finalidad	0	**6**
Minimización y Proporcionalidad	5	**5**
Plazo de Conservación	1	**0**
Consentimiento	4	**1**
Responsable	2	**4**
Encargado	1	**3**
Corresponsable	1	**0**
Derechos	3	**0**
Tratamientos Videocámaras	1	**0**
Categorías Especiales de datos	13	**6**
Seguridad en el Tratamiento	0	**4**
Delegado Protección Datos	3	**0**
Transparencia y acceso a registros públicos	6	**0**
Telecomunicaciones	12	**3**
Menores	4	**2**
Administración electrónica	0	**5**
Códigos de conducta	1	**1**

Nota: *Existen consultas que versan sobre más de una materia y que por su relevancia constan en más de un apartado.*

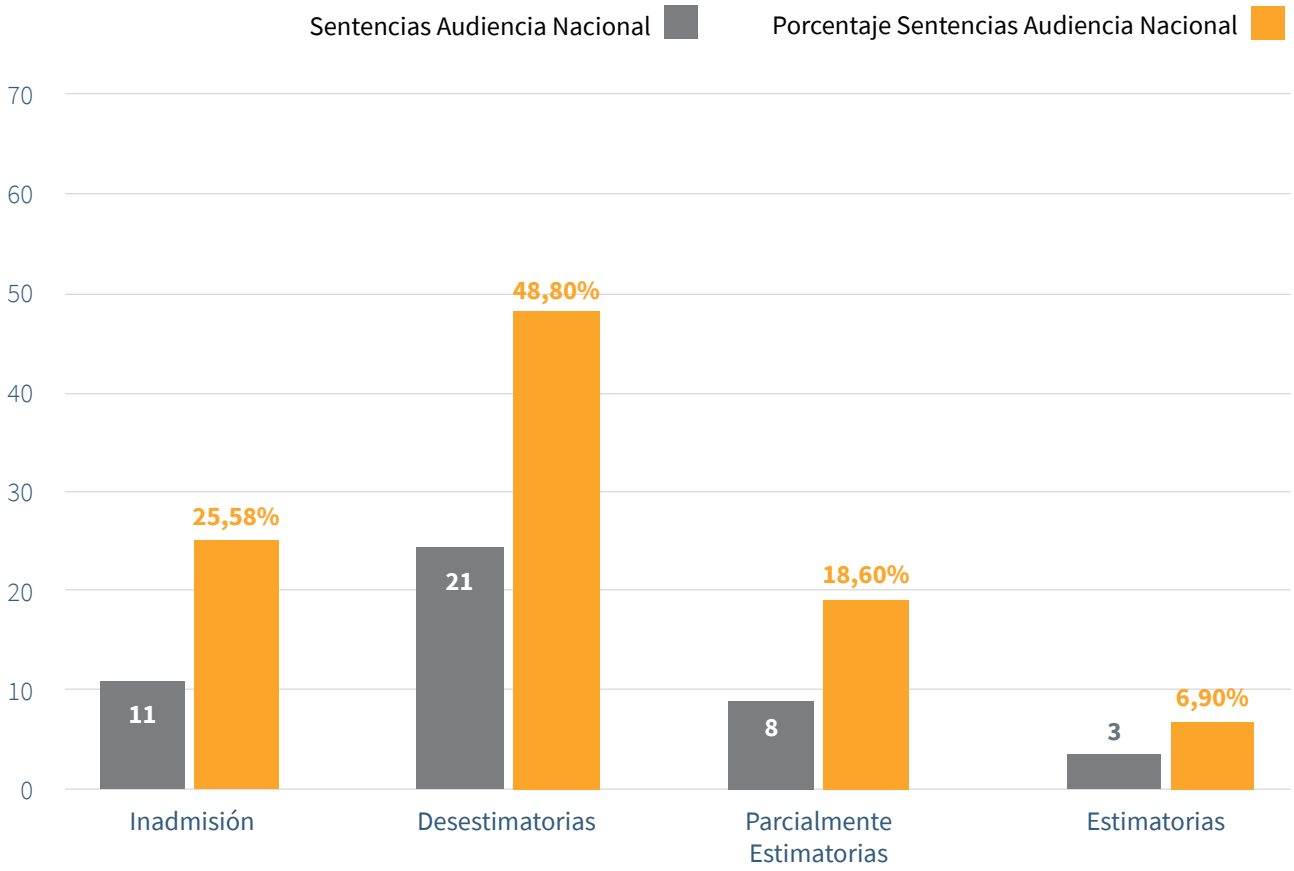
*** **Conceptos Generales:*** *se incluyen aquí las consultas sobre proyectos de disposiciones generales.*

Evolución informes preceptivos (2014 - 2024)			
Año	Disposiciones generales	RD 424/2005	Total
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
2023	49	8	57
2024	**38**	**2**	**40**

Evolución de informes preceptivos a disposiciones generales (2014-2024)



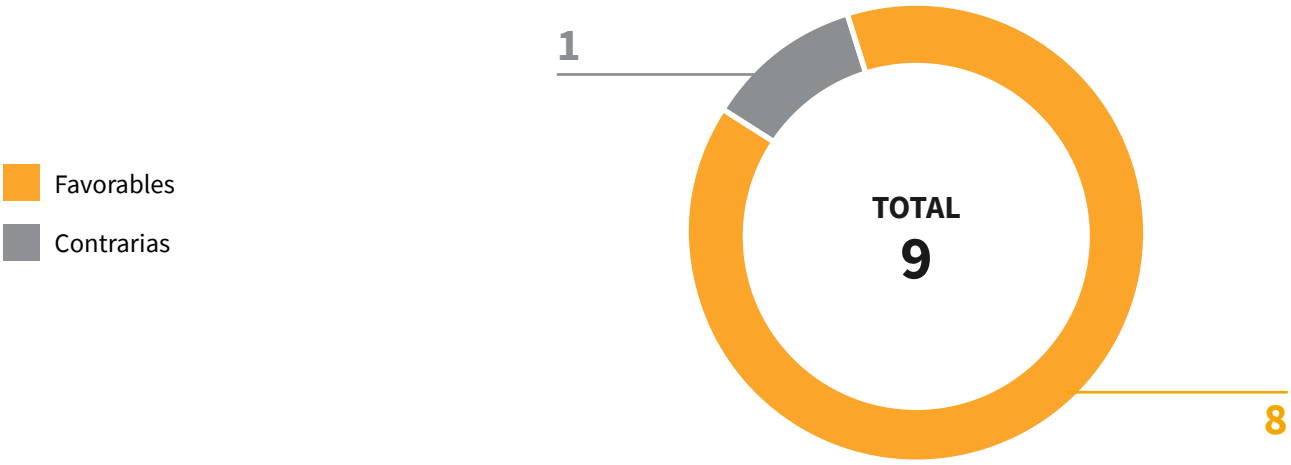
Sentencias Audiencia Nacional 2024



TOTAL* Sentencias Audiencia Nacional	**43**

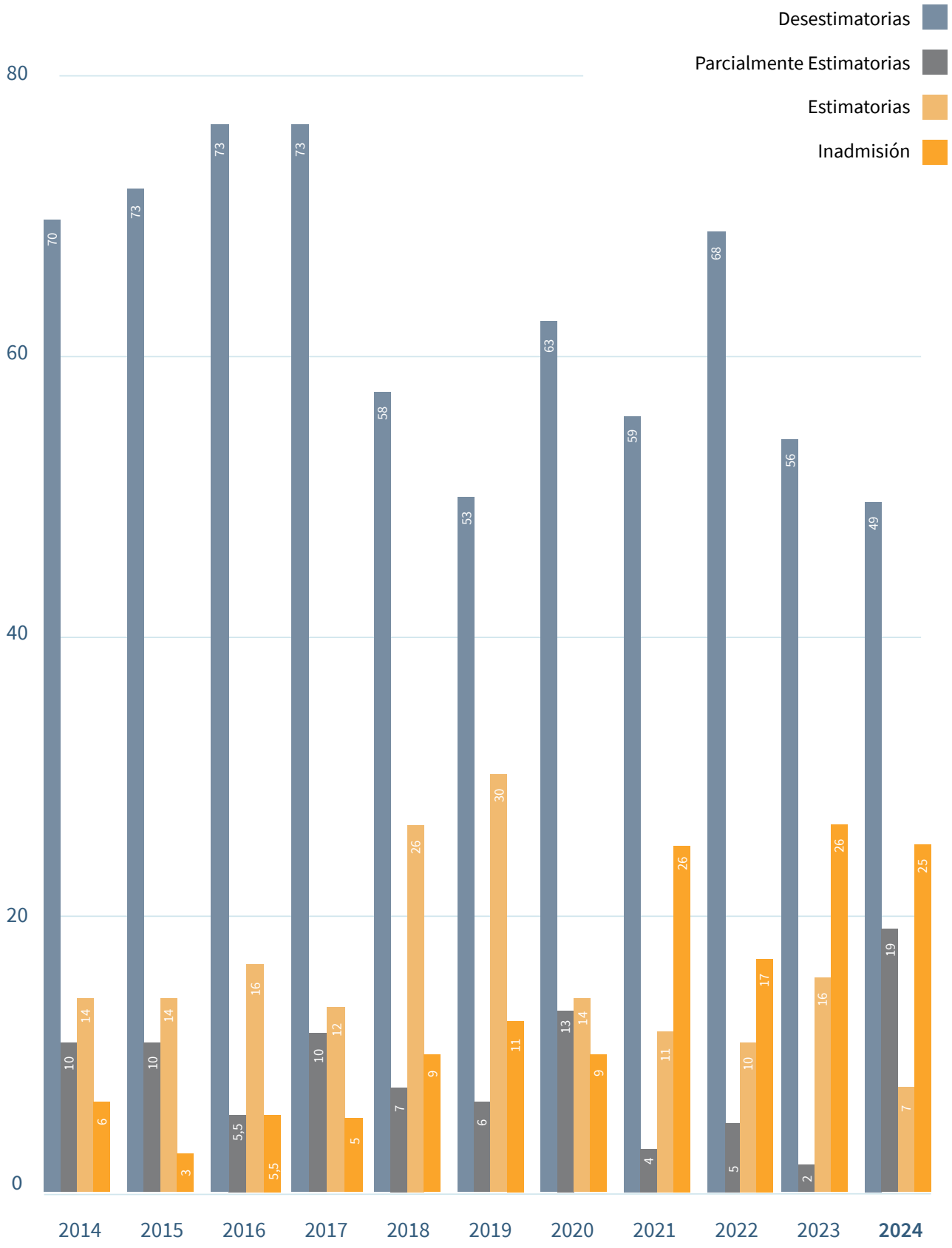
***Nota:** se incluyen Sentencias de 2023 notificadas en 2024 para dar continuidad a la Memoria del ejercicio anterior.*

Sentencias Tribunal Supremo (2024)



Evolución por sentido del fallo (AN) en porcentajes (2014 - 2024)				
Ejercicio (año)	Desestimatorias	Parcialmente Estimatorias	Estimatorias	Inadmisión
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
2023	56	2	16	26
2024	**49**	**19**	**7**	**25**

Evolución por sentido del fallo (AN) en porcentajes (2014 - 2024)



Comparativa por sector recurrente (2023 - 2024)		
	2023	2024*
Particulares	42	**28**
Banca y seguros	2	**2**
Telecomunicaciones	2	**6**
Solvencia patrimonial y crédito	0	**2**
Distribución y venta	0	**1**
Agua y energía	3	**2**
Administraciones Públicas	0	**1**
Otros	6	**4**
Asociaciones y sindicatos	2	**2**
Sociedad de la información	2	**0**
Salud	4	**0**
TOTAL	63	**48**

Nota* *En este ejercicio se incluyen únicamente sentencias de la AN y del TS (no autos, decretos de desestimiento, etc.,)*

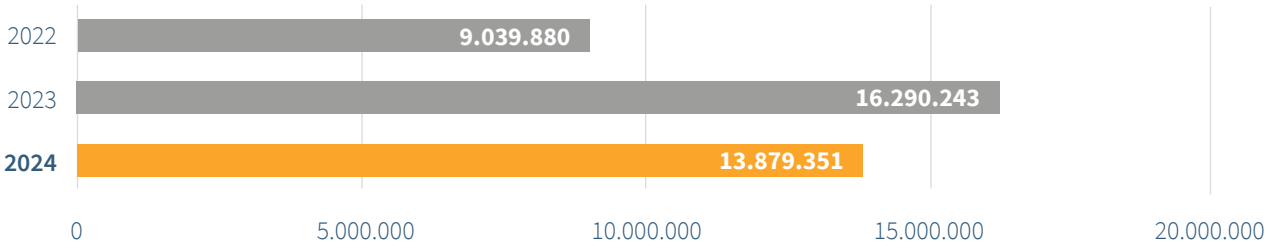
3. Atención al ciudadano y sujetos obligados

Consultas totales planteadas ante el área de Atención al Ciudadano				
	2022	2023	2024	% 2023-2024
Presenciales	110	189	308	62,96%
Telefónicas	42.562	46.958	51.374	9,40%
Sede electrónica y email	3.766	4.397	3.991[1]	-9,23%
Consultas servicio Chatbot[2]		17.337	42.489	145,08%
TOTAL	**46.438**	**68.881**	**98.162**	**42,51%**

[1] *Incluye las consultas del canal de atención al ciudadano (3.046); así como las quejas y sugerencias 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 (221); y también las consultas del canal DPD (724).*

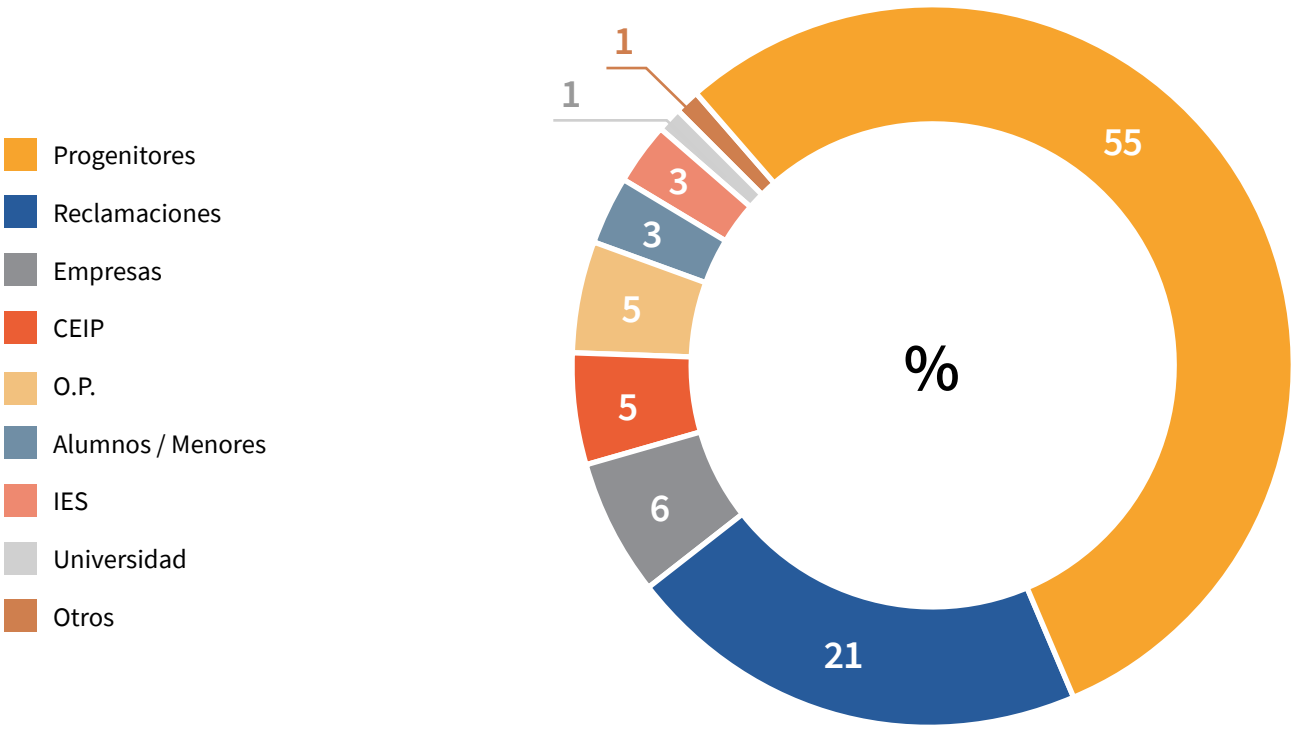
[2] *Es un servicio permanente (24x7) de respuesta inmediata con posibilidad de derivar a un agente. Disponible en la web desde el 12 de abril de 2023.*

Comparativa de visitas a la web (*www.aepd.es*)				
	2022	2023	2024	% 2023-2024
Nº de visitas	9.039.880	16.290.243	13.879.351	-14.80%



Consultas específicas sobre el tratamiento de datos de menores	
	2024
Teléfono	2.291
WhatsApp	639
Correo-e	501
Sede electrónica	161
TOTAL	**3.592**

Consultas por categorías[3] (en porcentajes)



[3] Este gráfico está elaborado con las consultas recibidas en el Área de Educación y Menores, a través de los cuatro canales de consulta, a excepción de las llamadas no relacionadas con el Área.

Accesos a la web www.tudecideseninternet.es	
	2024
Número de visitas	319.205

Canal del DPD				
Consultas	2022	2023	2024	% 2023-2024
	695	850	724[4]	-14.82%

[4] *A través de la sede electrónica (556) y derivadas de otros canales (168).*

Informe de Accesos a FAQ	
	Nº de visitas
Reglamento General de Protección de Datos. (RGPD)	173.392
Cuestiones sobre la sede electrónica	104.706
Comunidades de Propietarios	86.057
Menores y educación	81.361
Solvencia patrimonial (ficheros de morosos)	77.528
Tratamiento de datos en el Ámbito Laboral	71.320
Reclamaciones ante AEPD y ante otros organismos competentes	69.856
Tus Derechos (Información, Acceso, Rectificación y Cancelación)	65.554
Delegado de Protección de Datos	55.010
Videovigilancia	49.752
Transparencia y protección de datos	32.344
Transferencias internacionales, BCR y Códigos de conducta	28.623
Canal Prioritario para contenidos sensibles en internet	28.265
Procesos electorales	16.280
Publicidad no deseada	11.576
Internet y Redes Sociales	9.642
Salud	8.656
TOTAL	**969.922**

Áreas temáticas	
Áreas de actuación	**Nº de visitas**
Educación y Menores (Canal Joven)	319.205
Internet y redes sociales	156.687
Canal prioritario	100.069
Salud	90.691
Videovigilancia	88.963
Publicidad no deseada	87.737
Reclamaciones de telecomunicaciones	70.397
Administraciones públicas	65.821
Violencia de género	46.243
Innovación y tecnología	34.926

Temas más consultados en la atención telefónica			
Orden	Temas de consulta	2023	2024
1	Reclamaciones	11.570	**12.711**
2	Reglamento general de protección de datos (RGPD)	8.211	**8.597**
3	Derechos	5.503	**5.608**
4	Videovigilancia	3.965	**4.920**
5	Ficheros de solvencia patrimonial	1.898	**1.906**
6	Cuestiones técnicas de la sede electrónica	1.023	**1.509**
7	Comunidades de propietarios	1.239	**1.408**
8	Herramienta FACILITA	1.180	**1.171**
9	Delegados de Protección de Datos	1.089	**916**
10	Tratamiento de datos en el ámbito laboral	630	**758**
11	Transparencia y Protección de Datos	77	**39**
12	Otras cuestiones	3.875	**6.202**

Canal de consulta-web con respuesta inmediata 24 horas | CHATBOT			
Orden	Categorías de consulta	2024	%
1	Reclamaciones ante la AEPD	8.209	19,32
2	Tus derechos	7.638	17,98
3	Publicidad no deseada	4.994	11,75
4	Videovigilancia	4.319	10,17
5	Reglamento general protección de datos	3.679	8,66
6	Ficheros de morosos	3.584	8,44
7	Internet y redes sociales	2.816	6,63
8	Protección de datos en el ámbito laboral	2.032	4,78
9	Comunidades de propietarios	1.964	4,62
10	Salud	1.557	3,66
11	Educación y menores	1.264	2,98
12	Canal prioritario para contenidos sensibles en internet	431	1,02

Otros contenidos	
Guías	**Descargas**
Guía sobre el uso de las cookies	**183.729**
Guía para centros educativos	**85.208**
Guía sobre el uso de videocámaras para seguridad y otras finalidades	**68.775**
La guía que no viene con el móvil	**63.935**
Guía sobre tratamientos de control de presencia mediante sistemas biométricos	**59.156**
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	**52.710**
La protección de datos en las relaciones laborales	**43.785**
Responsabilidades y obligaciones en la utilización de dispositivos digitales móviles en la enseñanza (publicada en la web el 17/09/24)	**42.519**
Estrategia de Menores, salud digital y privacidad (publicada en la web el 29/01/24)	**40.724**
Guía para la notificación de brechas de datos personales	**33.639**
Guía para el responsable de tratamiento de datos personales	**29.923**
Guía de Protección de Datos por Defecto	**29.757**
Guía de Privacidad y Seguridad en Internet	**29.553**
Directrices para la elaboración de contratos entre responsables y encargados del tratamiento	**28.192**
Uso de cookies para herramientas de medición de audiencia (publicada en la web el 11/01/24)	**24.705**
Hoja de ruta para garantizar la conformidad con la normativa de protección de datos	**24.011**
Guía para el cumplimiento del deber de informar	**23.971**
Protección de datos y Administración Local	**22.972**
Patrones adictivos en el tratamiento de datos personales (publicada en la web el 10/05/24)	**22.960**
Guía para pacientes y usuarios de la Sanidad	**20.930**
Decálogo de Principios. Verificación de edad y sistemas de protección de personas menores de edad ante contenidos inadecuados	**20.462**

Otros contenidos	
Guías	**Descargas**
Compra segura en INTERNET - Guía Práctica	**19.576**
Guía para el ciudadano	**19.032**
Tecnologías de seguimiento WIFI: Orientaciones para responsables del tratamiento (publicada en la web el 07/05/24)	**17.757**
Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial	**15.880**
Guía de Privacidad desde el diseño	**14.536**
Listado de elementos para el cumplimiento normativo	**14.127**
Guía de protección de datos y prevención de delitos	**13.397**
Guía para profesionales del sector sanitario	**12.479**
Guía de administradores de fincas	**12.318**
Orientaciones y Garantías en los procedimientos de anonimización	**12.054**
Nota técnica de las pruebas de concepto sobre sistemas de verificación de edad	**8.246**
Requisitos para Auditorías de Tratamientos que incluyan IA	**8.220**
Drones y Protección de Datos	**7.793**
Código de buenas prácticas en protección de datos para proyectos Big Data	**7.029**
Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo	**6.916**
Utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas	**6.668**
Informe utilización por profesores y alumnos de aplicaciones que almacenan datos en nube...	**6.668**
Guía de protección de datos y prevención de delitos: fichas prácticas	**5.928**
Orientaciones para la validación de sistemas criptográficos en la protección de datos	**5.732**
La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD	**5.452**

Otros contenidos	
Guías	**Descargas**
Guía de Tecnologías y Protección de Datos en las AA.PP.	**5.418**
Aproximación a los espacios de datos desde la perspectiva del RGPD	**5.364**
Risk Management and Impact Assessment in the Processing of Personal Data	**4.917**
Guía para clientes que contraten servicios de Cloud Computing	**4.876**
A Guide to Privacy by Design	**4.394**
10 malentendidos relacionados con la anonimización	**4.287**
Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales	**3.121**
FAQ de las pruebas de concepto sobre sistemas de verificación de edad	**3.029**
RGPD compliance of processings that embed Artificial Intelligence An introduction	**2.813**
Cómo gestionar una fuga de información en un despacho de abogados	**2.468**
Orientaciones sobre cookies y analítica web en portales de las administraciones públicas	**2.336**
Decalogue of principles. Age verification and protection of minors from inappropriate content	**2.298**
Guía para la gestión y notificación de brechas de seguridad (versión en inglés)	**2.188**
Orientaciones para prestadores de servicios de Cloud Computing	**1.986**
Audit Requirements for Personal Data Processing Activities involving AI	**1.909**
Guidelines Clocking and Attendance Control Processing Using Biometric Systems	**1.770**
Anexo: Descripción técnica Prueba de Concepto Blockchain y el derecho de supresión (publicada en la web el 13/11/24)	**1.202**
Drones and Data Protection	**1.102**
Guidelines for Data Protection by Default	**992**
WI-FI Tracking Technologies: Guidance for Data Controllers (publicada en la web el 08/05/24)	**933**

Otros contenidos	
Guías	**Descargas**
Guidelines for the validation of cryptographic systems in data protection processing	**873**
Addictive patterns in the processing of personal data (publicada en la web el 10/05/24)	**856**
Technical note with the description of the Proofs of Concept of Systems for Age Verification	**844**
Guía sobre el uso de las cookies (versión en inglés)	**811**
10 Misunderstandings Related to Anonymisation	**714**
Guidelines for conducting a data protection impact assessment in regulatory development	**643**
Criterios de acreditación para los organismos de supervisión de códigos de conducta	**561**
Frequently Asked Questions about the Proofs of Concept of systems for age verification	**555**
10 Misunderstandings about Machine Learning	**541**
10 Malentendidos sobre el Machine Learning (Aprendizaje Automático)	**422**
Roadmap to ensure compliance with data protection regulation	**394**
Infografías	**Descargas**
Información sobre consentimiento para tratar datos personales de menores de edad	**23.933**
Responsabilidad de los y las menores (y de sus padres y madres) por los actos cometidos en Internet	**16.360**
Actuación del coordinador/a de bienestar y protección del alumnado	**14.837**
Riesgos asociados a sistemas de verificación de edad y resumen del decálogo de principios	**13.022**
Infografía Protección del menor en Internet	**11.931**
¿Cómo afectan las pantallas a la salud?	**11.327**
¿Qué debes tener en cuenta antes de dar un teléfono móvil a tu hijo o hija?	**10.776**
Decálogo sobre el impacto de la pornografía en niños, niñas y adolescentes (Publicada en la web el 30/09/24)	**10.473**
Derecho a no recibir llamadas comerciales no solicitadas	**10.060**

Otros contenidos	
Infografías	**Descargas**
Cuáles son tus derechos de protección de datos	**9.281**
Criterios para el tratamiento de datos personales en centros educativos	**8.619**
Quién es quién en el tratamiento de datos personales en tu centro educativo	**5.951**
Plan digital familiar	**5.672**
Cuándo y cómo se debe comunicar una brecha de datos a los afectados	**4.873**
Mapa de referencia para tratamientos que incluyen Inteligencia Artificial	**4.771**
Decálogo para el personal sanitario y administrativo	**4.679**
Recomendaciones para usuarios en la utilización de chatbots con Inteligencia Artificial	**4.625**
Los derechos que tienes para proteger tus datos personales	**4.578**
Infografía: Medidas para minimizar el seguimiento en internet	**4.372**
Compra segura en internet	**3.956**
10 consejos básicos para comprar en internet de forma segura	**2.831**
Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada	**2.783**
Riesgos del internet de las cosas en el hogar	**2.771**
Cumple con la normativa y #protege sus datos	**1.587**
Juguetes conectados	**1.568**
Infografía: El control es tuyo, que no te controlen	**1.438**
Protección de datos en vacaciones	**1.406**
Cómo evitar la publicidad no deseada	**1.325**
Reglamento de Protección de Datos	**1.262**
Recomendaciones en la contratación a distancia de servicios de telecomunicaciones y energía	**1.144**

Otros contenidos	
Infografías	**Descargas**
Recommendations for users in the use of chatbots with artificial intelligence	**1.136**
Facilita Emprende	**1.116**
Denuncia la difusión de contenidos violentos o sexuales en Internet	**1.061**
Canal Prioritario - Igualdad	**999**
Balance Plan Estratégico	**947**
Risks associated with age verification systems and summary of the Decalogue of principles	**718**
Reference Map Personal data processing embedding Artificial Intelligence	**644**
Notas técnicas	**Descargas**
Introducción a las tecnologías 5G y sus riesgos para la privacidad	**9.424**
Protección del menor en Internet	**7.842**
Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo	**7.138**
Medidas para minimizar el seguimiento en internet	**6.924**
Introducción a LIINE4DU 1.0: una nueva metodología para el modelado de amenazas para la privacidad y la protección de datos (Publicada en la web el 24/10/24)	**5.906**
La K-anonimidad como medida de la privacidad	**3.769**
Internet seguro por defecto para la infancia (Publicada en la web el 02/10/24)	**3.476**
14 equívocos con relación a la identificación y autenticación biométrica	**3.118**
El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles	**2.680**
Prueba de concepto Blockchain y el derecho de supresión (Publicada en la web el 13/11/24)	**2.266**
K-anonymity as a privacy measure	**1.166**
El uso de las tecnologías en la lucha contra el COVID19	**1.138**

Otros contenidos	
Notas técnicas	**Descargas**
Patrones adictivos y el derecho a la integridad de la persona (Publicada en la web el 16/12/24)	**819**
Control del usuario en la personalización de anuncios en Android	**795**
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”	**791**
Privacidad en DNS	**719**
Recomendaciones para el despliegue de aplicaciones móviles en el acceso a espacios públicos	**606**
A safe Internet by default for children (Publicada en la web el 02/10/24)	**474**
DNS Privacy	**315**
Introduction to 5G technologies and their risks in terms of privacy	**297**
An introduction to LIINE4DU 1.0: a new privacy&data protection threat modelling framework (Publicada en la web el 24/10/24)	**289**
Otras publicaciones	**Descargas**
Fingerprinting o Huella digital del dispositivo	**11.416**
Adecuación a la normativa a ‘coste cero’ y otras prácticas fraudulentas	**5.492**
Introducción al hash como técnica de seudonimización de datos personales	**5.399**
Informe sobre políticas de privacidad en internet. Adaptación al RGPD	**5.094**
Orientaciones para la aplicación de la disposición adicional octava y la disposición final duodécima de la LOPDGDD	**4.214**
Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles	**2.957**
Decálogo para la adaptación al RGPD de las políticas de privacidad en internet	**2.743**
Preguntas frecuentes sobre la anulación del Escudo de Privacidad	**2.065**
Introduction to the Hash function as a personal data pseudonymisation technique	**1.996**
25 años de la Agencia Española de Protección de Datos	**1.981**

Otros contenidos	
Otras publicaciones	**Descargas**
Encuesta sobre el grado de preparación de las empresas españolas ante el RGPD (AEPD-CEPYME)	**1.925**
LOPD: Novedades para el Sector Privado	**1.614**
Plan de inspección de oficio de la atención sociosanitaria	**1.530**
LOPD: Novedades para los ciudadanos	**1.107**
FAQ sobre el COVID-19	**1.104**
LOPD: Novedades para el Sector Público	**902**
Análisis de los flujos de información en Android	**895**
Plan de inspección sectorial de oficio Hospitales Públicos	**849**
Survey on Device Fingerprinting	**550**
Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía	**488**
Memorias	**Descargas**
Memoria AEPD 2023	**7.743**
Memoria de Responsabilidad Social 2023	**1.941**

Pacto digital para la protección de personas

Pacto digital para la protección de personas	
	2024
Entidades adheridas (totales)	555

Códigos de Conducta [5]						
	Aprobados	Modificados	Inadmitidos	Archivados	En tramitación	Iniciativas
2024	1	0	0	4	9*	10
Total códigos de conducta aprobados						**1**

** Cuatro códigos son de carácter transnacional, en uno de ellos la AEPD actúa como correvisor.*

[5] 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.

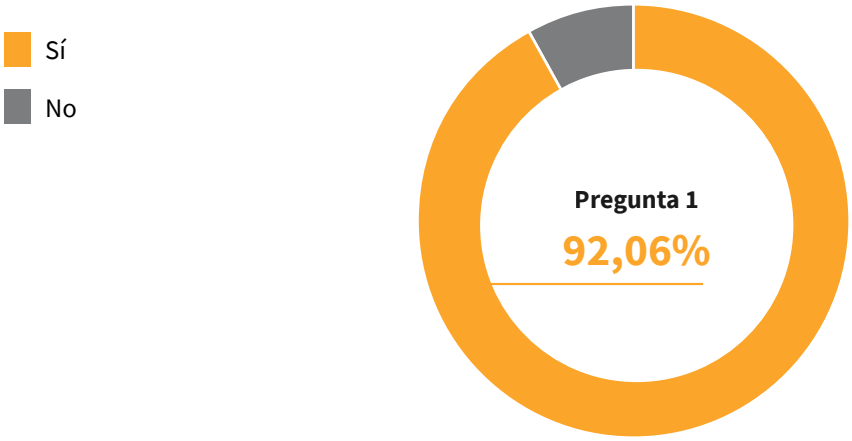
Encuestas de calidad de la atención telefónica 2024			
Resumen general		**SI**	**NO**
1	¿Está satisfecho con el contenido de la información recibida?	3.965	342
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	3.974	333
3	¿Está satisfecho con la corrección en el trato por parte del operador?	4.094	213
Total de encuestas contestadas		**4.307**	

Análisis de respuestas		**SI**	**NO**
1	¿Está satisfecho/a con el contenido de la información recibida?	92,06%	7,94%
2	¿Considera que la persona que le atendió tiene los conocimientos técnicos suficientes?	92,27%	7,73%
3	¿Está satisfecho/a con la corrección en el trato por parte del operador?	95,05%	4,95%
Total de encuestas contestadas		**100%**	
Promedio de satisfacción		**93,15%**	

Encuestas de Calidad

Número Total 4.307

¿Está satisfecho con el contenido de la información recibida?

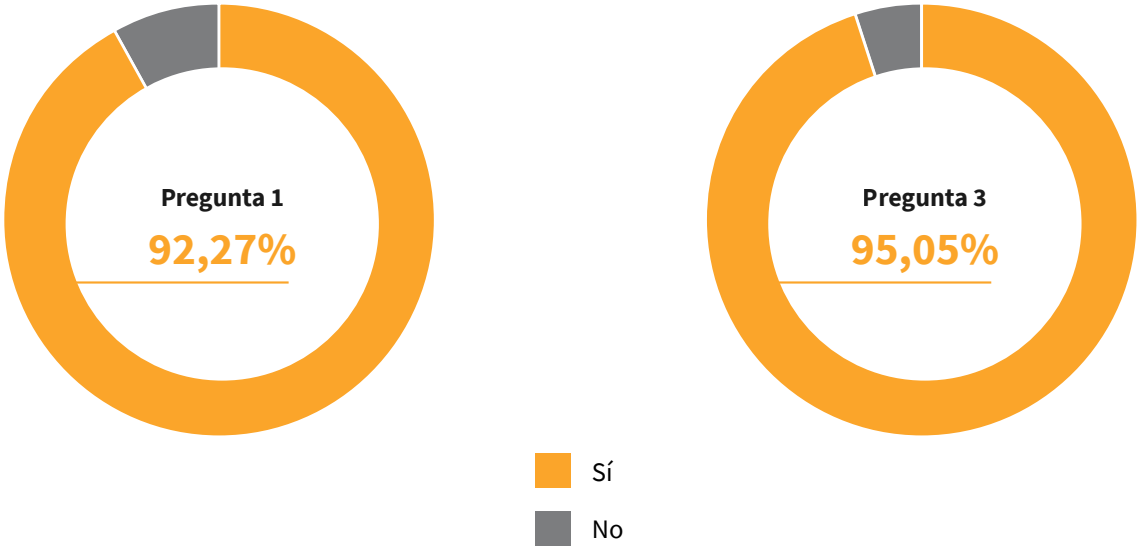


Encuestas de Calidad

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?



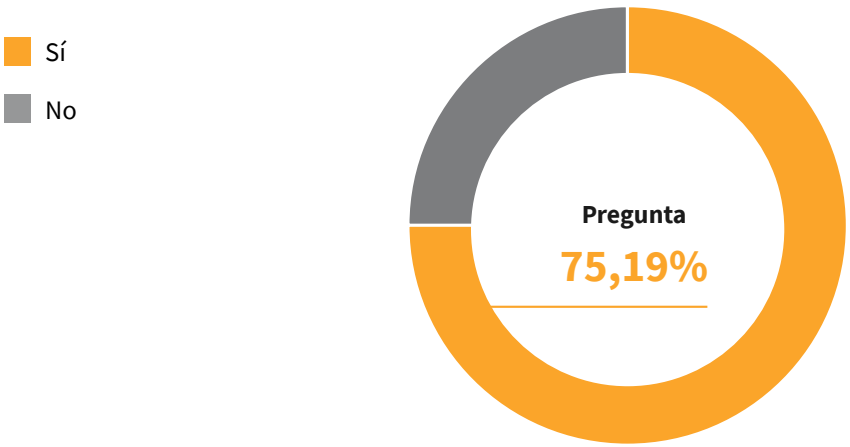
Encuestas de Satisfacción del Chatbot 2024		
Resumen general	**SI**	**NO**
1 Queremos saber su opinión sobre el servicio. ¿Le hemos ayudado?	1.618	534
Total de encuestas contestadas	**2.152**	

Análisis de respuestas	**SI**	**NO**
1 Queremos saber su opinión sobre el servicio. ¿Le hemos ayudado?	75,19%	24,81%
Total de encuestas contestadas	**100%**	
Índice de Satisfacción del Cliente	**75,19%**	

Encuestas de Satisfacción

Número Total 2.152

Queremos saber su opinión sobre el servicio. ¿Le hemos ayudado?



Accesos a la sección de transparencia			
2022	2023	2024	% 2023-2024
127.549	173.463	259.245	49,45 %

Solicitudes de acceso a la información pública						
Año	Solicitudes	Concedidas	Inadmitidas	Concedidas parcialmente	Denegadas	Desistidas
2024[6]	158[7]	78	53[8]	11	6	9

[6] *Siete resoluciones corresponden a expedientes de diciembre 2023.*

[7] *Un expediente en tramitación.*

[8] *Inadmitidas incluye: Devueltas a Unidad Central 4 y finalizaciones anticipadas (por acumulación u otras causas, 14).*

Reclamaciones ante el CTBG			
Año	Reclamaciones	Estimatorias	Desestimatorias
2024	16[9]	1	10[10]

Registro de Delegados de Protección de Datos comunicados[11]		
Titularidad		Total notificados
Entidades Privadas		109.853
Entidades Públicas		9.950
	Administración General del Estado	209
	Comunidades Autónomas	480
	Entidades Locales	5.121
	Otras personas Jurídico-Públicas - Consejo General del Poder Judicial - Notarios - Colegios Profesionales - Universidades - Cámaras de Comercio - Comunidades Regantes	4.140
TOTAL		**119.803**

[9] *Cinco pendientes de resolución*

[10] *Desestimatorias incluye Archivadas 2 e Inadmitidas 1*

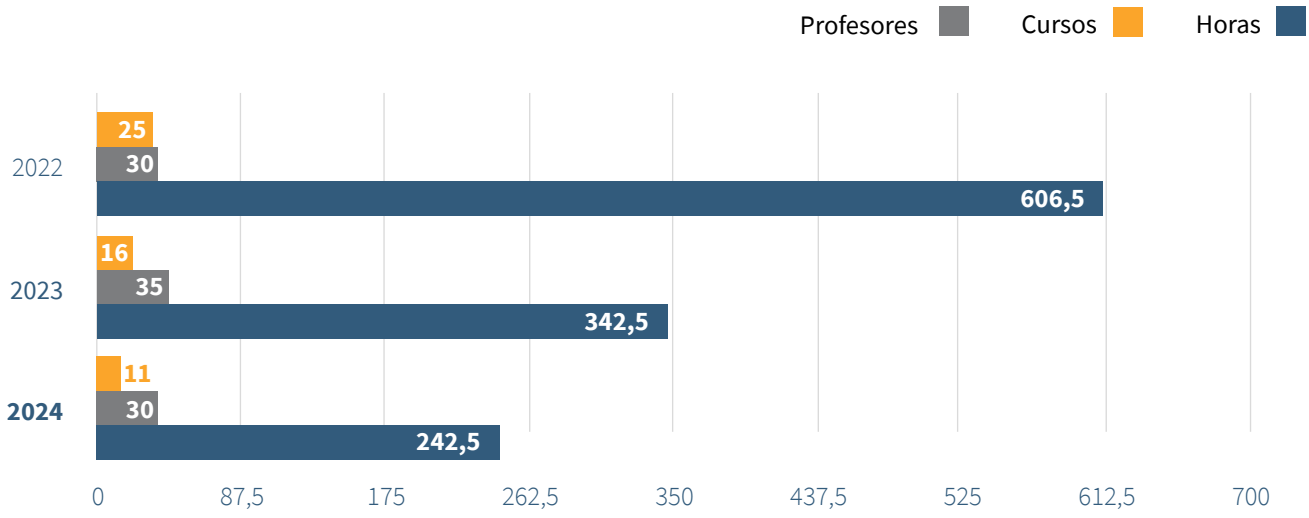
[11] *Durante 2024 se han atendido 628 consultas e incidencias relativas a la comunicación de los DPD y se han recibido un total de 19.024 comunicaciones de Delegados de Protección de Datos.*

Transferencias Internacionales desde 2019		
	2024	Total acumulado
Autorizaciones de transferencias internacionales	-	1 (Art. 46.3.b RGPD)
Normas Corporativas Vinculantes (BCR) adoptadas por la AEPD	5	16
Normas Corporativas Vinculantes (BCR) en tramitación por la AEPD como autoridad líder	5	-
Normas Corporativas Vinculantes (BCR) en las que la AEPD ha participado como co-revisora	4	41

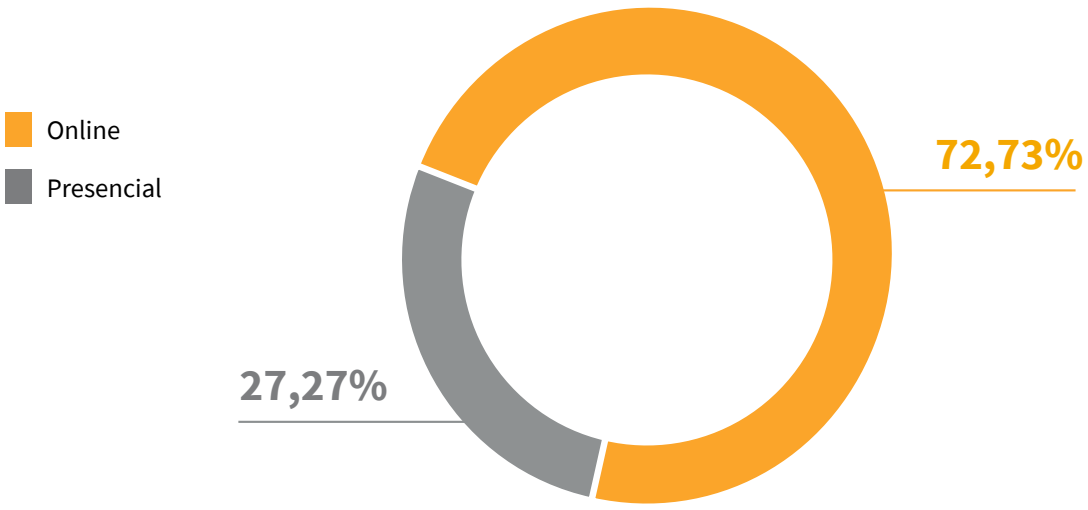
Esquema de Certificación de DPD (AEPD-DPD)			
	2022	2023	2024
Auditorías	4	3	5
Revisión de preguntas de examen	3.932	3.696	4.245
Elaboración de exámenes	72	78	66
Seguimiento de entidades de formación	136	324	231
Seguimiento de entidades de certificación	15	14	15
Reconocimiento de formación universitaria	1	1	0
DPD Certificados	138	169	206
Total DPD Certificados			**1.306**

Formación[12]			
	2022	2023	2024
Cursos	25	16	**11**
Profesores	30	35	**30**
Horas	606,5	342,5	**242,5**

[12] Coordinadas por la Subdirección General de Promoción y Autorizaciones.



Formato del curso



A continuación, se detallan las actividades formativas que la AEPD ha desarrollado a lo largo del año 2024, cuya gestión se ha realizado desde la Subdirección General de Promoción y Autorizaciones.

Cursos Generales de Protección de Datos (formato online o presencial)

Organismo	Fechas	Duración	Formato	Nº alumnos
M. Defensa (Ejército Tierra)	15/01 - 30/01	20 h	Online	60
M. Defensa (Armada)	05/02 - 20/02	20 h	Online	60
Ministerio de Sanidad	15/04 - 18/04	20 h	Online	20
Ministerio del Interior	11/06 - 14/06	20 h	Presencial	30
M. Defensa (Subsecretaría)	17/09 - 03/10	20 h	Presencial	70
M. Presidencia, Justicia y Relaciones con las Cortes	14/10 - 21/10	15 h	Online	28
M. Política Territorial y Memoria Democrática	04/11 - 14/11	20 h	Presencial	15
M. Trabajo y Economía Social	12/11 - 14/11	10 h	Online	25

Cursos Generales de Protección de Datos (formato Moodle)

Organismo	Fechas	Duración	Nº alumnos
M. Defensa (Ejército Tierra)	05/02 - 17/03	6 semanas	60
M. Defensa (Armada)	26/02 - 14/04	6 semanas	60
M. Transportes y Movilidad Sostenible	01/04 - 12/05	6 semanas	35
M. Defensa (Subsecretaría)	07/10 - 17/11	6 semanas	70

Jornadas y otros cursos

Organizado por	Fecha	Denominación	Ponencia
Plataforma de ONG de Acción Social	31 / 01	Jornada 'Protección de datos personales y desarrollo organizacional en organizaciones sociales'	Protección de Datos Personales en las entidades sociales.
JEF Spain	02 / 02	DIRECT- Your Digital Rights	Understanding Digital Rights and Privacy
Escuela Diplomática	13 / 02	VI Curso de Especialización en Servicio Exterior	Protección de los Datos Personales en el Exterior
ISMS Forum	12 / 06	Gestión y Automatización de Solicitudes de Acceso del Interesado	Ejercicio de derechos y solicitudes de acceso
Ministerio Industria y Turismo	25 / 09	Curso acceso escala titulados superiores de OO.AA.	Política de protección de datos de carácter personal en la AGE
Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP) como parte implementadora	16 - 18 julio	Jornadas de Concienciación Regional sobre la Protección de Datos en el Sector Salud (Costa Rica)	La protección de datos en ámbito de la salud
Jornada APEP	18 / 09	El DPO como pieza clave de los nuevos equipos de gestión de datos	La figura del DPD
León Research S.L.	26 / 09	Farmaforum 2024	Ensayos descentralizados, el reto de la verificación remota de los datos fuentes de un ensayo clínico
Centro de Referencia Estatal de atención al Daño Cerebral-CEADAC	27 / 09	Jornadas Protección de Datos	Ley de Protección de Datos y Comunicación entre profesionales
Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP) como parte implementadora	30 / 09 01 / 10	Diálogo Político de Alto Nivel en Protección de Datos, de la iniciativa Alianza Digital UE-ALC (Montevideo – Uruguay)	Transferencias Internacionales de Datos

Jornadas y otros cursos

Guardia Civil	15 / 10	I Jornada de seguridad de la información y protección de datos	Modelos de gestión de protección de datos y seguridad de la información
	16 / 10	I Jornada de seguridad de la información y protección de datos	Aspectos éticos, disciplinarios y administrativos
ISMS Forum	14 / 11	XXVI Jornada Internacional de Seguridad de la Información	La evolución del DPD en el marco de los derechos digitales
Centro de Estudios Jurídicos	15 / 11	Curso selectivo 46ª promoción Cuerpo Letrados Admón. Justicia	Protección de datos personales
Wolters Kluwer Legal Software	12 / 12	Webinar Legal Innovation Days	El derecho a la protección de datos personales en el ejercicio de la abogacía

Cursos en el entorno educativo y de menores

Organizado por	Fecha	Denominación	Ponencia
Universidad de Murcia	08 / 02	Jornada Protección de Datos y Menores (Murcia)	Líneas de acción de la AEPD para la protección de los menores en el entorno digital
Generalitat de Cataluña	21 / 03	Jornada 'Cómo proteger a los niños, niñas y adolescentes del acceso a la pornografía en el ámbito digital' (Barcelona)	La legislación española sobre la protección de la infancia y la adolescencia
Secretaría de Estado de Seguridad (Ministerio del Interior)	09 / 04 07 / 05	II Jornadas Formativas sobre Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos	Protección del Menor en la Internet de las cosas
Asociación Aragonesa de delegados de protección de datos	16 / 04	III Jornadas Aragonesas de Protección de Datos, Transparencia y Ciberseguridad (Calatayud)	El móvil en las aulas

Cursos en el entorno educativo y de menores

Consejería de Desarrollo Educativo y FP (Junta de Andalucía)	17 / 06	Jornada efectos negativos que las pantallas están teniendo en el desarrollo psicológico y social de la infancia y la adolescencia (Sevilla)	Privacidad y Salud Digital
Fundación Cursos de Verano de la Universidad del País Vasco	25 / 06	Curso de verano: Digitalización de la enseñanza: una visión desde la protección de datos (San Sebastián)	Privacidad y Salud Digital
Pantallas Amigas, Universidad de Deusto y Asociación de Internautas	27 / 06	Jornada Videojuegos y derechos digitales de la infancia (Bilbao)	Protección de los derechos de las personas menores en los entornos digitales desde la AEPD
Pantallas Amigas	07 / 10	Jornada 'Inteligencia artificial y derechos de la infancia en el contexto digital'	Menores y derechos digitales
Universidad Rey Juan Carlos	08 / 10	IV Congreso Internacional sobre Menores y medios sociales: identidades digitales vulnerables y controles de contenidos en salud emocional	Moderación, regulación y autorregulación en redes sociales y medios
Defensor del Pueblo Andaluz	09 / 10	Jornada 'Derechos en Red. Por un espacio digital seguro para la infancia y adolescencia' (Cádiz)	Privacidad, Educación y Salud Digital
Fundación Atresmedia	19 / 10	3er Encuentro para profesores Mentes AMI	La protección de los derechos digitales de niños y jóvenes
Asociación Multidisciplinar y de Investigación sobre la Infancia y Parentalidad Positiva (ASEMIP)	25 / 10	IX Congreso ASEMIP 2024 'Infancia y parentalidad positiva: prevención de la violencia y Adicciones en línea' (Cuenca)	Conferencia de Clausura
Fundación Plan B y Ayuntamiento de Zamora	12 / 11	4ª Semana de la Infancia y la Adolescencia (Zamora)	Derecho del menor a la intimidad y protección de datos
INTEF	3,4 / 12	Congreso Nacional de Competencia Digital Educativa (Valladolid)	Protección de datos en el centro educativo AEPD: Protección de datos en educación

Cursos en el entorno educativo y de menores

Universidad Autónoma de Madrid	03 / 12	Jornadas Infancia	Seguridad e Infancia
Asociación Profesional Española de Privacidad (APEP)	12 / 12	La patria potestad digital y el acceso a los contenidos de los dispositivos digitales de los menores por parte de sus progenitores	
Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)-Uruguay	12 / 12	Jornada Protección de los menores en el ámbito digital y el Canal Prioritario	Protección de los menores en el ámbito digital y el Canal Prioritario

Jornadas sobre violencia digital hacia las mujeres y el Canal Prioritario

Solicitado por	Fecha	Denominación
Red Iberoamericana de Protección de Datos (Costa Rica)	29 / 02	Iniciativas de Autoridades de Protección de datos en Iberoamérica Costa Rica-Canal Prioritario
Ayuntamiento de Bormujos (Sevilla)	14 / 03	Curso 'La violencia de género digital, otra forma de violencia de género'
Policía Nacional	07 / 05	I Curso de Derechos Humanos e Igualdad de Género-Policía Nacional
Instituto de las Mujeres (Mº de Igualdad) y Universidad de Salamanca	10 / 05	Repensando el elemento tecnológico en clave de igualdad: hacia el humanismo digital (Salamanca)
Delegación del Gobierno de las Islas Baleares	04 /10	I Jornada sobre Violencia Sexual (Palma de Mallorca)
Policía Nacional	20 / 11	II Curso de Derechos Humanos e Igualdad de Género
Ayuntamiento de Iznalloz (Granada)	03 / 12	Jornadas técnicas 'Violencia de Género en el Entorno Digital 'Realidad y Herramientas para Prevenir'

Cursos que se programan e imparten para el personal al servicio de la Administración Pública a través del INAP

Denominación	Fecha	Nº de alumnos
Curso Básico RGPD en AA.PP.	Febrero y marzo	300
Programa de Especialización para DPDs de las AA.PP.	De febrero a junio	60
Curso Básico RGPD en AA.PP.	Octubre y noviembre	300

Jornadas organizadas en la AEPD

Curso Menores y Redes Sociales, dirigido a Fiscales. Organizado con la Fiscalía General del Estado y el Centro de Estudios Jurídicos	19 y 20 de febrero
Visita de alumnos de la Universidad de Suffolk (EEUU): Interesados en conocer las implicaciones del GDPR para las empresas estadounidenses, así como el nuevo marco transatlántico para las transferencias internacionales de datos UE/EEUU. Charla impartida por el Departamento de Internacional.	12 de marzo
II Sesión informativa con alumnos de la facultad de Derecho de Stetson University de Florida, sobre la protección de datos personales en el ámbito laboral.	4 de junio
Visita del Instituto de Acceso a la Información Pública de Honduras (IAIP)	25 de noviembre
Visita Comité Marroquí para el Derecho de Acceso a la Información (CDAI)	3 de diciembre
Jornada 'Cinco años de Responsabilidad Social y Protección de la Infancia y la Adolescencia en el entorno online'	16 de diciembre

Asistencia a eventos

Gala de entrega del Premio internacional de la 17ª edición de los Quality Innovation Award (QIA), celebrado en Zhuhai City (China), otorgado en la categoría 'Innovación en sector público' por el proyecto de la AEPD 'Iniciativas prácticas para proteger a los menores en internet con entornos saludables, positivos y seguros'	11 de abril
Rueda de Prensa - Vamos a hablar de pornografía, Ministerio de Igualdad	7 de octubre

AGENDA INSTITUCIONAL

Durante 2024 la Agencia continuó con su misión de fomentar entre ciudadanos y organizaciones la cultura de la protección de datos, así como de contribuir al 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.

La relación completa y detallada de la agenda institucional de la AEPD puede consultarse en la siguiente **sección web**.

11 de enero	**Reunión del Grupo de Trabajo de Menores, Salud Digital y Privacidad**
15 de enero	**Inauguración de la nueva sección de Infancia y Adolescencia del ICAM**
16 de enero	**Reunión plenaria del Comité Europeo de Protección de Datos**
16 de enero	**Ciclo de conferencias 'El triple reto de los móviles en educación: Salud, Seguridad y Convivencia'**
17 de enero	**Reunión con empresas de telecomunicaciones y DigitalES**
17 de enero	**Gala de entrega de Premios SEIS**
18 de enero	**Reunión con representantes de Microsoft**
18 de enero	**Reunión con representantes de Amazon**
23 de enero	**Reunión con representantes de la Asociación Española de Videojuegos**
23 de enero	**Reunión de la Task Force de la Comisión Europa encargada del Reglamento de Servicios Digitales**
23 de enero	**Reunión bilateral con la Autoridad de Protección de Datos del estado de California**
23 de enero	**Reunión bilateral con la Agencia Federal de Comercio de Estados Unidos**
24 de enero	**Webinario sobre Protección de Datos de la ULACIT**
24 de enero	**Reunión con representantes de Incibe**
29 de enero	**Presentación de la Estrategia de la AEPD sobre menores, salud digital y privacidad**
29 de enero	**Inauguración de la nueva sección de Protección de Datos del ICAM**
30 de enero	**Reunión con la secretaria de Estado de Igualdad y para la Erradicación de la Violencia contra las Mujeres**

AGENDA INSTITUCIONAL

31 de enero	Jornada 'Protección de datos personales y desarrollo organizacional en organizaciones sociales'
31 de enero	Reunión con la directora general de Derechos de la Infancia y Adolescencia
31 de enero	Reunión con representantes de Apple
31 de enero	Debate sobre la respuesta judicial a la ciberviolencia que sufren las mujeres y los y las menores
1 de febrero	Jornada 'El valor de los medios de comunicación en el nuevo orden tecnológico mundial. Periodismo y empresas' de UTECA
5 de febrero	Reunión del Grupo de Trabajo de Menores, Salud Digital y Privacidad
5 y 6 de febrero	Foro UNESCO sobre Inteligencia Artificial
7 de febrero	Reunión con representantes de Autismo España
8 de febrero	Jornada sobre la responsabilidad de los menores en el ámbito de la protección de datos
9 de febrero	State of AI 2024
12 de febrero	Reunión en el Ministerio de Justicia
13 de febrero	Jornada de presentación de la declaración para proteger a niños y adolescentes en el ámbito digital
13 de febrero	Reunión plenaria del Comité Europeo de Protección de Datos
14 y 15 de febrero	XXI Foro de Seguridad y Protección de Datos de Salud
19 y 20 de febrero	Curso 'Menores y redes'
19 de febrero	Comparecencia de la directora de la AEPD en el Parlamento de Andalucía
19 de febrero	Reunión Comité Ejecutivo RIPD
20 de febrero	Reunión con la eurodiputada Laura Ballarín
21 de febrero	Reunión de Autoridades de control de protección de datos
21 de febrero	XVI Foro de la Privacidad del ISMS Forum
23 de febrero	Reunión con el responsable de privacidad de la Casa Blanca
23 de febrero	Entrega de los Premios Fundación Zaballos

AGENDA INSTITUCIONAL

26 de febrero	Visita del Ministerio de Administraciones Públicas de la República Dominicana y el Banco Interamericano de Desarrollo
27 de febrero	5º encuentro del Espacio de Estudio sobre Inteligencia Artificial
27 de febrero	Reunión con representantes de Meta
27 de febrero	Despantallados: por una infancia y juventud libre y saludable
29 de febrero	Identidad, neurotecnologías, neurodatos, neuroderechos en el metaverso (XR)
4 de marzo	Encuentro con las plataformas de internet y el sector de las telecomunicaciones para la protección de los menores en el ámbito digital
11 a 13 de marzo	Visita del Centro Nacional para la Protección de Datos Personales de Moldavia
12 de marzo	Annual Executive Retreat 2024 del CIPL
12 de marzo	Reunión con Guido Scorza
12 de marzo	Reunión con representantes de las Autoridades de protección de datos y de Garantía de las Comunicaciones de Italia
12 de marzo	Sesión informativa con alumnos de la Universidad de Suffolk (Estados Unidos)
13 de marzo	Webinario 'Innovación y Protección de datos. Mujer y Ciencia'
14 de marzo	Reunión plenaria del Comité Europeo de Protección de Datos
14 de marzo	Curso 'La violencia de género digital, otra forma de violencia de género'
21 de marzo	Reunión de trabajo sobre el acceso por menores a contenidos online inapropiados
21 de marzo	Jornada 'Cómo proteger a los niños, niñas y adolescentes del acceso a la pornografía en el ámbito digital'
26 de marzo	Conferencia sobre protección de datos personales y violencia de género digital
1 a 3 de abril	Reunión de Grupos de Trabajo de la RIPD
9 de abril	II Jornadas formativas sobre 'Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos'
11 de abril	Gala de entrega de los premios QIA
16 de abril	III Jornadas Aragonesas de protección de datos, transparencia y ciberseguridad

AGENDA INSTITUCIONAL

16 de abril	I Mesa Tolerancia Cero contra el maltrato
16 de abril	Reunión con representantes de DigitalES, Ametic y fabricantes de dispositivos
16 y 17 de abril	Reunión plenaria del Comité Europeo de Protección de Datos
17 de abril	Evento 'Desmitificar la garantía de edad para los derechos del niño'
18 de abril de 2024	Encuentro con embajadores de América Latina ante la UE
24 de abril	Jornada Denaria 2024 'El efectivo: garantía de una transición digital justa, inclusiva y segura'
7 de mayo	I Curso de 'Derechos Humanos e Igualdad de Género-Policía Nacional'
10 de mayo	Congreso Internacional 'Repensando el elemento tecnológico en clave de igualdad: hacia el humanismo digital'
13 de mayo	Curso 'Salud Digital y Nuevas Tecnologías'
14 a 16 de mayo	Spring Conference 2024
14 de mayo	Jornada 'Las consecuencias de ser los primeros nativos digitales'
20 de mayo	Reunión plenaria del Comité de personas expertas para la generación de entornos digitales seguros
21 de mayo	Webinario 'Jóvenes, móviles y violencia de género'
23 de mayo	Reunión plenaria del Comité Europeo de Protección de Datos
27- 29 de mayo	XXI Encuentro anual de la Red Iberoamericana de Protección de Datos
27 y 28 de mayo	X Congreso Internacional de Privacidad de APEP
6 de junio	XI Congreso Internacional de Datos Personales
10 al 14 de junio	Privacy Symposium
10 de junio	Reunión extraordinaria del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia
12 de junio	Jornada 'Avances y retos en parentalidad positiva'
14 de junio	XVII Jornadas jurídicas de Sarriá 'Román García-Varela'
18 de junio	73ª reunión del Grupo de Berlín
20 de junio	Reunión plenaria del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia

AGENDA INSTITUCIONAL

24 de junio	Conferência Internacional 'Proteção de dados pessoais: ¿que futuro estamos a construir?'
24 de junio	Reunión plenaria del Comité Europeo de Protección de Datos
27 de junio	Reunión con representantes de la Fundación Mutua Madrileña y Atresmedia
10 de julio	La Agencia analiza los retos para la protección de las personas en Internet en los cursos de verano de la Universidad Menéndez Pelayo
15 de julio	Jornadas de Cooperación entre la AEPD, el INAI y la SEGIB
16 de julio	Reunión extraordinaria del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia
17 de julio	Reunión del Consejo Consultivo de la Agencia Española de Protección de Datos
19 de julio	Curso de verano UCM – Delegación del Gobierno contra la Violencia de Género: 'Pornografía y violencia sexual'
24 de julio	Reunión con el director general de derechos de las personas con discapacidad
24 de julio	Reunión del Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia
24 de julio	Reunión plenaria del Comité Europeo de Protección de Datos
2 de septiembre	Primer Congreso Internacional de Protección de Datos y Privacidad: Salud Digital y Privacidad de Menores
17 de septiembre	Reunión con representantes de Atresmedia
18 de septiembre	Presentación del estudio de la Fundación SOL sobre el impacto de los contenidos digitales en la infancia y la adolescencia
19 de septiembre	Plenario de la Fundación Hermes
19 de septiembre	Reunión de coordinadores de Grupos de Trabajo del Comité de personas expertas para la generación de entornos digitales seguros
24 de septiembre	Reunión plenaria del Comité Europeo de Protección de Datos
26 de septiembre	V Jornadas formativas sobre 'Trata y explotación sexual en entornos digitales'
26 de septiembre	Webinario de Nueva Mutua Sanitaria sobre protección de datos en el ámbito sanitario

AGENDA INSTITUCIONAL

26 de septiembre	Webinario sobre 'El impacto de la pornografía en el desarrollo afectivo-sexual de los menores'
27 de septiembre	Reunión de coordinadores de Grupos de Trabajo del Comité de personas expertas para la generación de entornos digitales seguros
30 de septiembre	Reunión con la presidenta de la Fundación Sol
1 de octubre	Diálogo Político de Alto Nivel en Protección de Datos
1 de octubre	Inauguración de la Comisión de Infancia y Juventud de Women in a Legal World
1 de octubre	ASSO DPO Congress Milán
3 de octubre	Reunión plenaria del Comité de personas expertas para la generación de entornos digitales seguros
3 de octubre	Reunión con el secretario de Estado de Economía y Apoyo a la Empresa
4 y 5 de octubre	Jornadas sobre nuevas tecnologías y educación
7 y 8 de octubre	Reunión plenaria del Comité Europeo de Protección de Datos
7 de octubre	Jornada 'Inteligencia artificial y derechos de la infancia en el contexto digital'
7 de octubre	Reunión plenaria del Comité de personas expertas para la generación de entornos digitales seguros
8 de octubre	IV Congreso Internacional sobre 'Menores y medios sociales: identidades digitales vulnerables y controles de contenidos'
9 de octubre	Jornada 'Derechos en Red. Por un espacio digital seguro para la infancia y adolescencia'
10 de octubre	Webinario 'Innovación y Protección de datos. Mujer y Ciencia' de la AEPD
10 de octubre	Reunión con representantes de la AEB
14 de octubre	Reunión plenaria del Comité de personas expertas para la generación de entornos digitales seguros
18 de octubre	Reunión con representantes de la AESIA
21 de octubre	II Semana de la Inteligencia Artificial.
24 de octubre	I Jornada sobre Violencia Sexual
25 de octubre	IX Congreso ASEMIP 2024 'Infancia y Parentalidad Positiva: Prevención de la Violencia y Adicciones en línea'

AGENDA INSTITUCIONAL

28 de octubre a 1 de noviembre	GPA 46th Global Privacy Assembly
30 de octubre	Reunión con la directora de la Secretaría de Derechos Digitales del Ministerio de Justicia y Seguridad Pública de Brasil
4 de noviembre	Reunión plenaria del Comité Europeo de Protección de Datos
12 de noviembre	IV Jornadas Tolerancia Cero de Mutua Madrileña
12 de noviembre	II Jornadas 'Principios de la Convención Derechos del Niño'
12 de noviembre	Reunión con representantes de Eurochild
12 de noviembre	Reunión con representantes de Fundación Sol y DigitalES
14 de noviembre	XXVI Jornada Internacional de Seguridad de la Información
16 de noviembre	XIII Curso para padres de adolescentes de Alicante
18 y 19 de noviembre	74º Encuentro del Grupo de Berlín
20 de noviembre	II Curso de Derechos Humanos e Igualdad de Género-Policía Nacional
25 de noviembre	Visita de una delegación de la IDLO en Honduras
2 y 3 de diciembre	Reunión plenaria del Comité Europeo de Protección de Datos
3 de diciembre	Jornadas Infancia
3 de diciembre	Jornadas técnicas Violencia de Género en el Entorno Digital 'Realidad y Herramientas para Prevenir'
3 de diciembre	Visita de estudio de una delegación del CDAI de Marruecos
3 y 4 de diciembre	Congreso Nacional de Competencia Digital Educativa
11 de diciembre	Sesión informativa a representantes de la AGESIC de Uruguay
12 de diciembre	Webinar Legal Innovation Days
12 de diciembre	Sesión Abierta de APEP sobre 'La patria potestad digital y el acceso a los contenidos de los dispositivos digitales de los menores por parte de sus progenitores'
17 de diciembre	Reunión plenaria del Comité Europeo de Protección de Datos

HERRAMIENTAS DE AYUDA DISPONIBLES EN LA WEB DE LA AEPD

Facilita RGPD[13]	
	2024
Accesos	36.261
Cuestionarios finalizados	14.903
Acumulados	**1.145.422**

[13] *Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales.*

Facilita EMPRENDE[14]	
	2024
Accesos	2.132
Cuestionarios finalizados	501
Acumulados	**20.832**

[14] *Facilita EMPRENDE, herramienta para ayudar a los emprendedores y startups tecnológicas a cumplir con la normativa de protección de datos.*

GESTIONA RGPD[15]	
	2024
Accesos	27.605
Cuestionarios finalizados	1.247
Acumulados	**52.974**

[15] *GESTIONA RGPD, herramienta orientada a los responsables y encargados del tratamiento, así como a los DPD, sobre aspectos básicos que se deben tener en cuenta, previamente a la realización de una adecuada gestión del riesgo para los derechos y libertades con relación a la protección de datos personales.*

EVALÚA-RIESGO RGPD[16]	
	2024
Accesos	21.823
Acumulados	**352.317**

[16] *Evalúa_Riesgo RGPD: herramienta 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.*

COMUNICA-BRECHA RGPD[17]	
	2024
Accesos	4.306
Cuestionarios finalizados	1.619
Acumulados	**21.012**

[17] *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.*

ASESORA-BRECHA RGPD[18]	
	2024
Accesos	7.705
Cuestionarios finalizados	2.451
Acumulados	**14.196**

[18] *Asesora-Brecha RGPD, recurso de utilidad para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de notificar sin dilación indebida a la Agencia Española de Protección de Datos una brecha de datos personales, tal y como establece el artículo 33 del Reglamento General de Protección de Datos*

ValidaCripto[19]	
	2024
Accesos	3.492
Cuestionarios finalizados	65
Acumulados	**7.578**

[19] ValidaCripto, herramienta dirigida a los responsables y encargados/ subencargados de tratamientos a los que se les aplique el RGPD o la LO 7/2021, que aplican criptografía en sus tratamientos de datos personales. Por lo tanto, también está orientada a los DPD, a los asesores en materia de protección de datos personales, a los auditores de protección de datos, a los especialistas en seguridad, y responsables funcionales de las entidades responsables o encargadas.

4. Brechas y consultas previas

Brechas de datos personales (Artículos 33 y 34 RGPD)	
Notificaciones de brechas de datos personales	**2.933**
Resoluciones para obligar a comunicar las brechas a los interesados	**13**
Traslados a la Subdirección General de Inspección de Datos	**15**
Número de interesados a los que los responsables han comunicado las brechas	**100.000.000**

Consultas previas (Artículo 36 RGPD)	
Consultas previas recibidas	**32**

5. Presencia internacional de la AEPD

Reunión	Fecha	Lugar
Sesiones Plenarias del Comité Europeo de Protección de Datos	16 de enero	Videoconferencia
	13 de febrero	Bruselas (Bélgica)
	14 de marzo	Videoconferencia
	16 y 17 de abril	Bruselas (Bélgica)
	23 de mayo	Videoconferencia
	18 y 19 de junio	Bruselas (Bélgica)
	16 de julio 7 de septiembre	Videoconferencia
	7 y 8 de octubre	Bruselas (Bélgica)
	4 de noviembre	Videoconferencia
	2 y 3 de diciembre	Bruselas (Bélgica)
	17 de diciembre	Videoconferencia
Reuniones de subgrupos del Comité Europeo de Protección de datos		
Subgrupo de asesoramiento (Strategic advisory- SAESG)	25 de enero 29 de enero 31 de enero 7 de febrero 29 de febrero 22 de marzo 27 de marzo 1 de julio 6 de septiembre 20 de septiembre 17 de octubre 14 de noviembre	Videoconferencia
	3 de diciembre	Reunión Híbrida

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Grupo de trabajo Cookie Banners	29 de abril	Videoconferencia
Medios Sociales Digitales (Social Media - SOCM)	23 de febrero 12 de abril	Videoconferencia
	28 de mayo	Bruselas (Bélgica)
	27 de junio 27 de septiembre	Videoconferencia
	5 de diciembre	Bruselas (Bélgica)
Cooperación (COOP)	1 de febrero	Bruselas (Bélgica)
	10 de abril 26 de junio 17 de julio 2 y 3 de septiembre 18 de septiembre	Videoconferencia
	26 de septiembre	Bruselas (Bélgica)
	5 de noviembre 17 de diciembre	Videoconferencia
Asuntos financieros (Financial Matters - FMES)	24 de enero 21 de febrero 21 de marzo 22 de abril 21 de mayo 18 de julio 22 de octubre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Transferencias internacionales (International Transfers - ITS)	17 de enero 6 y 7 de febrero	Videoconferencia
	5 y 6 de marzo	Bruselas (Bélgica)
	2 y 3 de abril 14 y 15 de mayo 11 de junio 2 y 3 de julio 25 de julio	Videoconferencia
	10 y 11 de septiembre	Bruselas (Bélgica)
	23 de septiembre 24 de septiembre 9 de octubre 5 y 6 de noviembre 4 de diciembre	Videoconferencia
Grupo de trabajo Multas (Fining – TF FINING)	1 de febrero 12 de marzo	Videoconferencia
	24 de abril	Bruselas (Bélgica)
	4 de julio 19 de septiembre 24 de octubre 9 de diciembre	Videoconferencia
Fronteras, viajeros y aplicación legislativa (BTLE)	25 de enero	Videoconferencia
	21 de marzo	Bruselas (Bélgica)
	28 de mayo	Videoconferencia
	4 de julio	Bruselas (Bélgica)
	26 de septiembre 7 de noviembre 29 de noviembre	Videoconferencia
	12 de diciembre	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Disposiciones clave (Key Provisions - KEYP)	9 de enero 30 de enero 15 de febrero	Videoconferencia
	7 de marzo	Bruselas (Bélgica)
	15 de marzo 20 de marzo 4 de abril 9 de abril 2 de mayo	Videoconferencia
	3 y 4 de julio	Bruselas (Bélgica)
	25 de julio 18 de septiembre 23 de septiembre 2 de octubre 14 de octubre 24 y 25 de octubre	Videoconferencia
	21 y 22 de noviembre	Bruselas (Bélgica)
	10 de diciembre	Videoconferencia
Supervisión del cumplimiento (Enforcement - ENF)	30 y 31 de enero	Bruselas (Bélgica)
	19 de marzo 22 de mayo 25 de junio	Videoconferencia
	24 y 25 de septiembre	Bruselas (Bélgica)
	7 de noviembre 22 de noviembre 4 de diciembre 18 de diciembre	Videoconferencia

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Usuarios de sistemas de información del CEPD (IT Users)	11 de marzo	Videoconferencia
	10 de junio	Bruselas (Bélgica)
	20 de septiembre 12 de diciembre	Videoconferencia
Tecnología (TECH)	17 y 18 de enero	Bruselas (Bélgica)
	12 de febrero 5 de marzo 13 de marzo 15 de abril 19 de abril 23 de abril	Videoconferencia
	14 de mayo	Bruselas (Bélgica)
	12 de junio 10 de julio 10 y 11 de septiembre	Videoconferencia
	23 de septiembre	Bruselas (Bélgica)
	14 de octubre	Videoconferencia
	24 y 25 de octubre	Bruselas (Bélgica)
	13 de noviembre	Videoconferencia
	20 y 21 de noviembre	Bruselas y remoto
	9 de diciembre	Videoconferencia
	10 de diciembre	Bruselas (Bélgica)

Reuniones de subgrupos del Comité Europeo de Protección de datos		
Reunión	**Fecha**	**Lugar**
Cumplimiento, Gobierno electrónico y Salud **(Compliance, E-goverment & Health - CEH)**	22 de enero	Videoconferencia
	22 de febrero 20 de marzo	Bruselas (Bélgica)
	11 de abril 18 de abril 24 de abril 7 de mayo 22 de mayo 30 de mayo	Videoconferencia
	25 de junio	Bruselas (Bélgica)
	19 de septiembre 25 de septiembre 22 de octubre 6 de noviembre	Videoconferencia
	19 de noviembre	Bruselas (Bélgica)
Grupo de Trabajo Chat GPT (TF- ChatGPT)	24 de enero 28 de febrero 27 de marzo 17 de abril 19 de junio 11 de septiembre 20 de noviembre	Videoconferencia
Grupo de Trabajo Competencia y Consumo **(Competition and Consumer Law – TF-C&C)**	19 de enero	Bruselas (Bélgica)
	20 - 22 de marzo 24 de abril 16 de mayo 19 de junio 17 - 19 de septiembre 27 de septiembre 15 de noviembre 6 de diciembre	Videoconferencia
Grupo de Trabajo Internacional (International Engagement TF-INT)	22 de enero 18 de marzo 21 de mayo 27 de mayo 22 de julio 16 de septiembre 15 de octubre 16 de diciembre	Videoconferencia

Control de Agencias y Grandes Sistemas de Información UE		
Reunión	**Fecha**	**Lugar**
Grupo de Supervisión Coordinada CSC (IMI, Eurojust, Europol, SIS, VIS)	19 - 20 de marzo	Bruselas (Bélgica)
	29 de mayo	Videoconferencia
	2 - 3 de julio	Bruselas (Bélgica)
	25 de septiembre 6 de noviembre	Videoconferencia
	10 - 11 de diciembre	Bruselas (Bélgica)
CIS	1 de julio 9 de diciembre	Bruselas (Bélgica)
EURODAC	1 de julio 9 de diciembre	Bruselas (Bélgica)
Evaluación Schengen	3 – 6 junio	Budapest (Hungría)

Consejo de Europa		
Comité Convención 108 (T-PD)	13 – 15 de marzo	París (Francia)
	5 – 7 de junio	Estrasburgo (Francia)
	11 – 12 de septiembre	Venecia (Italia)
	4 – 6 de noviembre	Estrasburgo (Francia)
Comité de Inteligencia Artificial (CAI)	23 al 26 de enero 11 al 14 de marzo 17 al 19 de septiembre 26 al 29 de noviembre	Estrasburgo (Francia)

Organisation for Economic Co-operation and Development (OECD)		
Working Party On Data Governance and Privacy (DGP)	27 y 28 de junio 8 de noviembre	París (Francia)
Promoting the Declaration on Government Access to Personal Data Held by Private Sector Entities	26 de septiembre	París (Francia)

Otras Reuniones		
Reunión	**Fecha**	**Lugar**
TAIEX Workshop on Raising awareness of Convention	26 de enero	Moldavia
UNESCO	5 – 6 de febrero	Eslovenia
European Data Innovation Board	7 de febrero	Luxemburgo
2nd Meeting of Working Group 3 (Data in Transit) of the HLG	13 de febrero	Bruselas
XXI Reunión del Foro de Seguridad y Protección de Datos de Salud (SEIS)	14 y 15 de febrero	Toledo
Parlamento Europeo	20 de febrero	Bruselas
Mobile World Congress	26 al 28 de febrero	Barcelona
22nd Annual Meeting of the Central and Eastern Europe Date Protection Authorities (CEEDPA)	28 de febrero – 1 marzo	Georgia
Protección de Datos y Violencia Digital de “Género”	26 de marzo	Cabo verde
BCR Workshop	8 –10 de abril	Lituania
1st Meeting of the Article 7 Subgroup of The High-Level Group for the Digital Markets ACT (EDPB)	20 de abril	Bruselas
Spring Conference	13 – 16 de mayo	Riga (Letonia)
International Conference in Zagreb	24 de mayo	Zagreb (Croacia)

Otras Reuniones		
Reunión	**Fecha**	**Lugar**
Privacy Symposium 2024	10 – 14 de junio	Venecia (Italia)
Encuentro Portugal 30 Aniversario CNPD	24 de junio	Lisboa (Portugal)
2024 Periodic Schengen Evaluation of Slovakia	6 – 11 de octubre	Viena
10 Asso DPO International Congress Milán	30 de septiembre - 01 de octubre	Milán (Italia)
Programme of the Inter-network meeting of data protection authorities (IRAPDP)	25 – 26 septiembre	Rabat (Marruecos)
Menkes & Other Rare Copper Diseases (MARCO I)	12 – 13 de septiembre	Málaga (España)
Data Protection Authorities Experience Exchange Forum	3 – 5 de septiembre	Varsovia (Polonia)
Grupo de Berlín	17 – 19 de junio	Oslo (Noruega)
	17 – 20 de noviembre	Bruselas (Bélgica)
Global Privacy Assembly	27 de octubre a 2 noviembre	Jersey
Best Practices GDPR-Supervision of Algorithms and AI	27 – 29 de noviembre	Holanda
European Genomic Data Infrastructure	8 de noviembre	Bruselas
European Case Handling Workshop	4 – 6 de diciembre	Estonia

Reuniones RIPD	
Reunión	**Nº de encuentros**
Organización para la Cooperación y el Desarrollo Económico (OCDE)	1
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)	3
Secretaría General Iberoamericana (SEGIB)	6
ISMS Forum	1
Programa de las Naciones Unidas para el Desarrollo (PNUD)	1
Agencia Española de Cooperación Internacional para el Desarrollo (AECID)	3
Foro Sociedad Civil de la RIPD	2
Agencia de Acceso a la Información Pública de Argentina (AAIP)	1
Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay (AGESIC)	1
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)	5
Agencia Andorrana de Protección de Datos (APDA)	1
Autoridad Nacional de Protección de Datos del Brasil (ANPD)	1
Instituto de Acceso a la Información Pública de Honduras (IAIP)	1
Agencia de Protección de datos de los Habitantes de Costa Rica (PRODHAB)	3
Fundación Internacional y para Iberoamérica De Administración Y Políticas Públicas (FIIAP)	4
Superintendencia de Protección de Datos Personales del Ecuador	1
Reuniones Comité Ejecutivo RIPD	1
Consejo Para La Transparencia de Chile (CPLT)	1
Secretaría de Derechos Digitales de Brasil	1
Superintendencia de Protección de Datos Personales del Colombia	1
Grupos de Trabajo de la RIPD en Lima (Perú)	1
Encuentro Anual RIPD Cartagena de Indias (Colombia)	1

6. Secretaría General

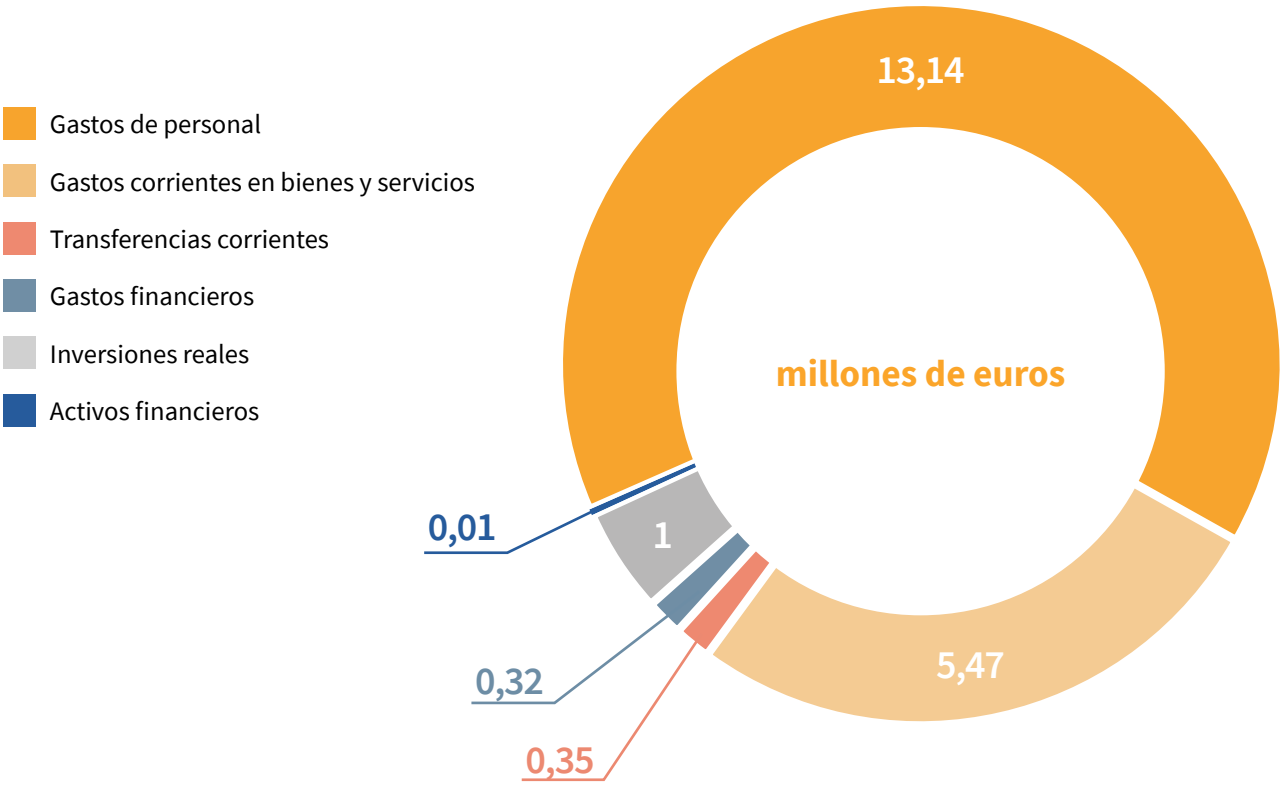
Evolución del presupuesto			
	Crédito Ejercicio		
	2022	2023	2024
Capítulo I	9.882.840	11.600.400	13.138.060
Capítulo II	5.359.840	5.468.240	5.468.240
Capítulo III	350.950	320.950	320.950
Capítulo IV	350.990	351.590	351.590
Capítulo VI	928.350	998.350	998.350
Capítulo VIII	11.200	11.200	11.200
TOTAL	**16.884.170**	**18.750.730**	**20.288.390**

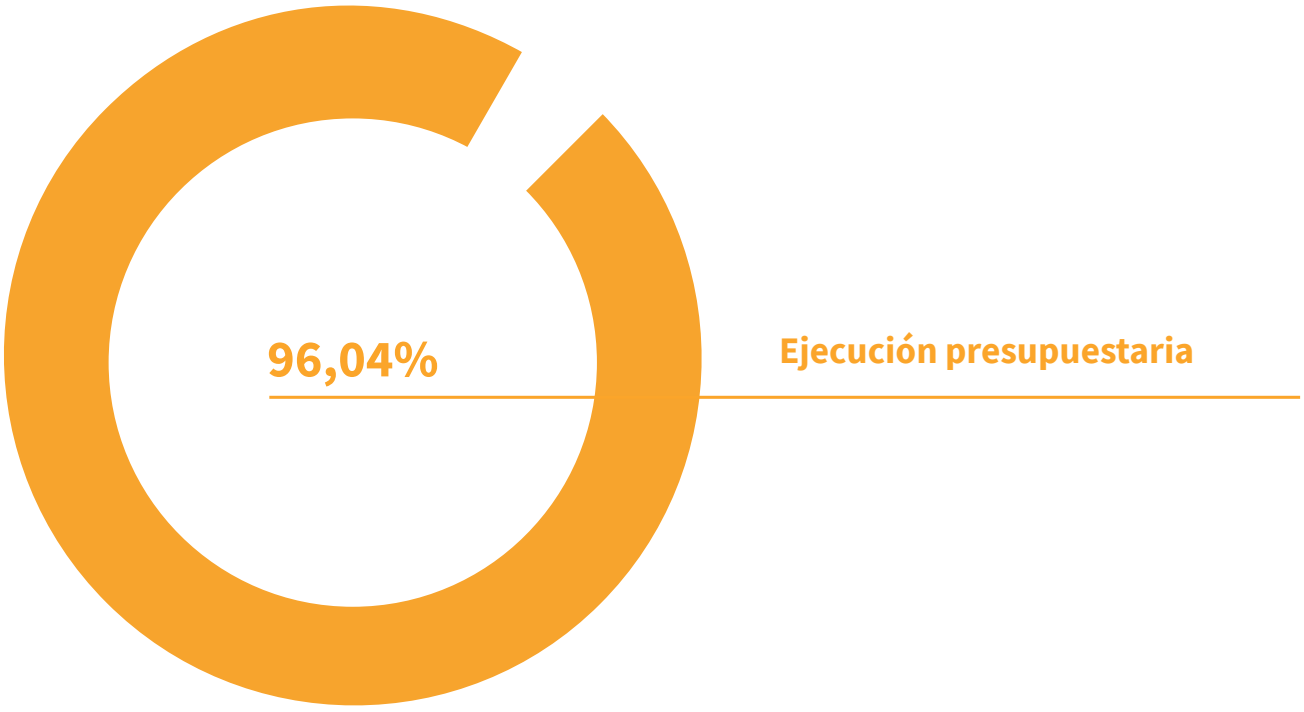
2024			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	13.138.059,88	12.810.725,12	97,51%
Gastos corrientes en bienes y servicios	5.468.240,00	5.056.548,02	92,47%
Gastos financieros	320.950,00	61.533,83	19,17%
Transferencias corrientes	351.590,00	207.580,00	59,04%
Inversiones reales	998.350,00	1.341.441,56	134,37%
Activos financieros	11.200,00	7.369,44	65,80%
TOTAL	**20.288.389,88**	**19.485.197,97**	**96,04%**

2023			
	Presupuesto definitivo	Obligaciones reconocidas	Porcentaje de ejecución
Gastos de personal	11.600.400,00	10.905.786,54	94,01%
Gastos corrientes en bienes y servicios	5.468.240,00	5.006.079,32	91,55%
Gastos financieros	320.950,00	1.128,38	0,35%
Transferencias corrientes	351.590,00	349.490,00	99,40%
Inversiones reales	998.350,00	1.216.948,08	121,90%
Activos financieros	11.200,00	4.825,80	43,09%
TOTAL	**18.750.730,00**	**17.484.258,12**	**93,25%**

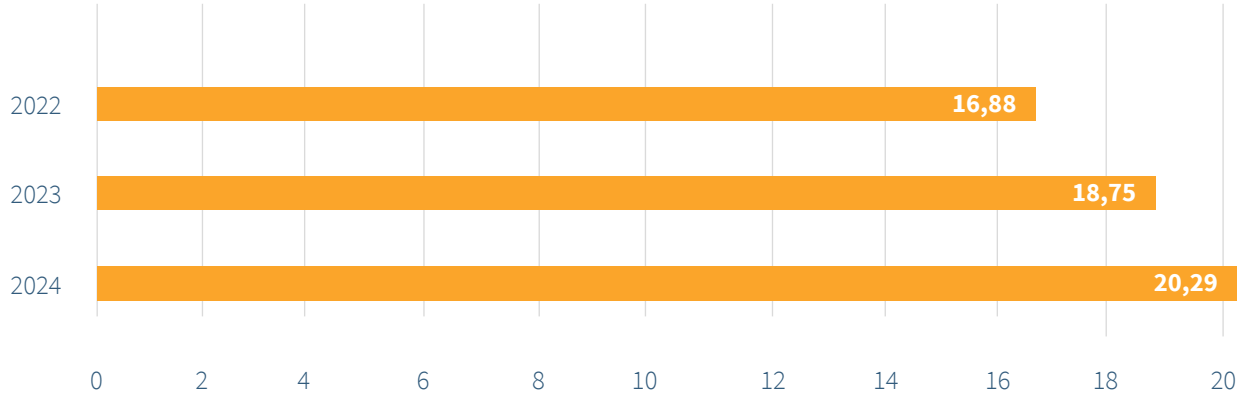
Diferencia 2024 - 2023		
	Presupuesto definitivo	Obligaciones reconocidas
Gastos de personal	1.537.659,88	1.904.938,58
Gastos corrientes en bienes y servicios	0,00	50.468,70
Gastos financieros	0,00	60.405,45
Transferencias corrientes	0,00	-141.910,00
Inversiones reales	0,00	124.493,48
Activos financieros	0,00	2.543,64
TOTAL	**1.537.659,88**	**2.000.939,85**

Distribución del presupuesto (en millones de euros)





Evolución del crédito presupuestario (millones de euros)

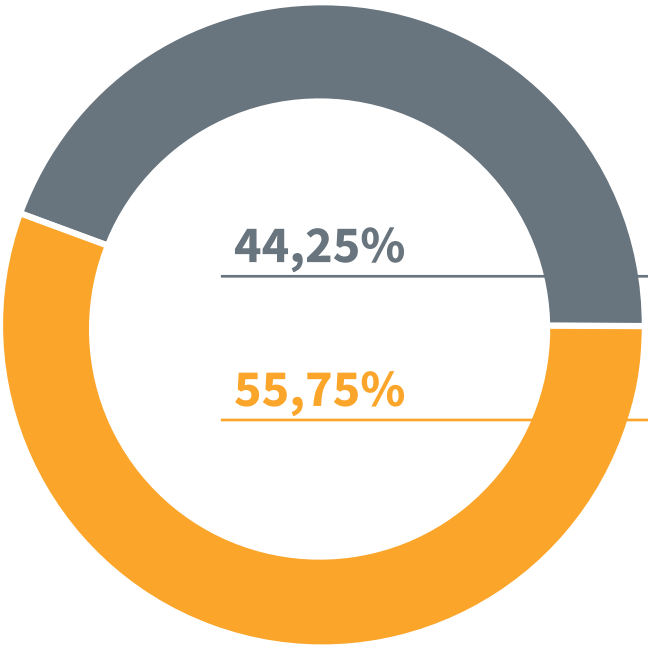


Gestión de recursos humanos a 31 de Diciembre 2024

	Dotación	Cubiertos
Funcionarios	241	216
Laborales	8	7
Laborales fuera de Convenio	2	2
Alto cargo	1	0*
TOTAL	**252**	**225**

La diferencia entre la dotación y la ocupación efectiva de puestos de personal funcionario se debe, principalmente, a que se incluyen puestos reservados a titulares que se encuentran ocupando otro puesto de trabajo, puestos creados para ser ocupados mediante oferta de empleo público, puestos de auxiliares de difícil cobertura y los puestos que están en proceso de toma de posesión tras la resolución del concurso específico convocado por Resolución de 30 de septiembre de 2024.

** El 24 de diciembre de 2024 la directora de la Agencia cesó en su puesto como titular de este organismo* **por Real Decreto del Consejo de Ministros**.



44,25% Hombres 100

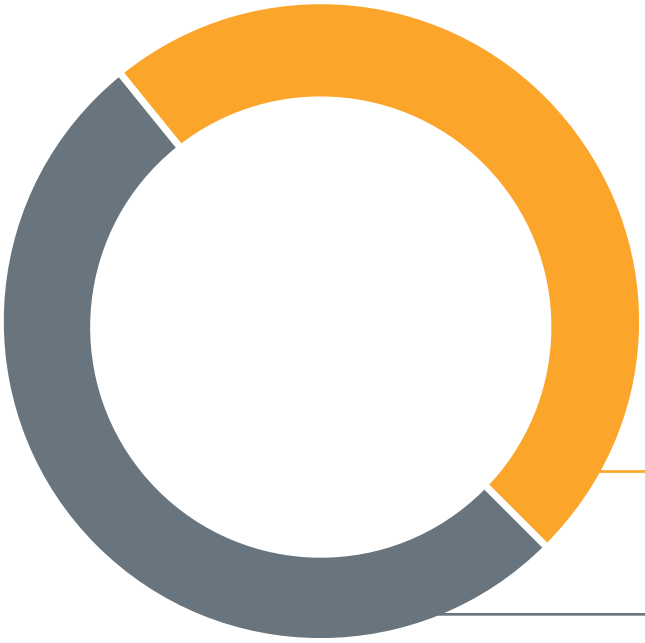
55,75% Mujeres 125

Personal funcionario												
Nivel	30	29	28	26	24	22	20	18	17	16	15	14
Efectivos	12	8	47	83	0	32	3	23	2	8	0	0

Grupo	A1	A2	B	C1	C2
Efectivos	70	82	1	41	22

División por niveles					
	Nivel 30	Nivel 29	Nivel 28	Nivel 26	TOTAL
Hombres	5	6	29	37	**77**
Mujeres	7	2	18	46	**73**
TOTAL	**12**	**8**	**47**	**83**	**150**

División por niveles



Antes de la aprobación del Plan de Igualdad de la AEPD en 2020, la Agencia contaba con un 61,54 % de hombres frente a un 38,46 % de mujeres en dichos puestos. A 31 de diciembre de 2024, dichos porcentajes se sitúan en un ***51,33% de hombres frente a un 48,67% de mujeres****, esto es, en tan solo 5 años se ha incrementado en 10 puntos la presencia femenina en los niveles directivos y pre directivos de la Agencia.*

Mujeres	**73**
Hombres	**77**

Evolución de la plantilla de Personal Funcionario y Laboral (RPT)

Año	Dotaciones
2018	186
2019	202
2020	202
2021	203
2022	217
2023	246
2024	252

www.aepd.es
AEPD_es
AEPD
@aepd.es